A Secured Quantum Two-Bit Commitment Protocol for Communication Systems

MANAL KHAWASIK1, WAGDY ELSAYED1, MAGDI RASHAD2, AND AHMED YOUNES1,3,4
1Department of Mathematics and Computer Science, Faculty of Science, Alexandria University, Alexandria 21544, Egypt
2Department of Computer Science, Faculty of Computers and Information Systems, Mansoura University, Mansoura 35516, Egypt
3School of Computer Science, University of Birmingham, Birmingham B15 2TT, U.K.
4Alexandria Quantum Computing Group, Faculty of Science, Alexandria University, Alexandria 21544, Egypt
Corresponding author: Manal Khawasik (manal.khawasik@alexu.edu.eg)

ABSTRACT Bit commitment is an essential primitive in quantum cryptography. It is the basic building block of many cryptographic protocols in which it provides security over distrustful parties. This paper proposes a secured quantum two-bit commitment protocol for any two classical bits. The protocol contains two parties - a committer and a receiver - who share both quantum and classical communication channels. The main phases of this protocol are commitment and revealing phases where the concealing and binding conditions are proved in order to accept the commitment message. The proposed framework utilizes different security layers to hide specific quantum states in a superposition alongside trivial one qubit operations. The secured unitary transformations are applied by the two parties to meet the concealing and binding conditions. To verify the success of the proposed protocol, the measured output of the two parties are compared. The protocol operates under the assumption that the two parties might cheat and the possible existence of an eavesdropper.

INDEX TERMS Quantum communication, quantum cryptography, quantum teleportation, quantum two-bit commitment.

I. INTRODUCTION Quantum Computing (QC) has become a promising tool to enhance the current technologies. It has affected many areas such as machine learning, optimization problems, material synthesis, and communication systems [1]–[4]. In communication systems, Bit commitment (BC) is the basic building block of many cryptographic protocols, for instance, it is widely used in multi-party-based secure computations such as verified secret sharing schemes [5]. It is used in the access control of cloud computing as it preserves the users’ privacy and provides a robust hiding access control policy [6]. The bit commitment is considered as a protocol between two distrustful parties - the committer Alice and the receiver Bob. It was first proposed by Blum in 1983 [7].

BC consists of two main phases known as commitment and revealing. In the commitment phase, Alice transmits a message to Bob who receives it without the ability to decode it until Alice permits that in the revealing phase [7]. The security of the BC protocol dictates the verification of both binding and concealing conditions. This means that Alice is not supposed to be able to change the bit she committed (binding) after the commitment phase, while Bob can not identify the bit that Alice has already committed until she reveals it (concealing) [8]. Due to the no-go theorem [9], the possibility of building a classical BC under various security conditions such as classical BC under relativistic settings, tamper-evident seals, or transmitting measurement outcomes started to be discussed [10], [11]. Theoretically, the current classical BC protocols can not achieve the unconditional level of security, one solution for this problem is inspired by the concept of quantum cryptography where the Quantum Bit Commitment (QBC) protocol is developed with higher levels of security [8], [12].

On the other hand, the first QBC scheme was proposed by Bennett and Brassard in 1984 [13], the protocol they described claimed to implement a coin-tossing problem. The main idea of QBC is inherited from the classical BC security primitives. It aims to improve the security of the communication systems and is used in cheating detection [14]. In 1990, Brassard et al. implemented the bit commitment with more modifications in order to overcome the predictable EPR (Einstein– Podolsky– Rosen) attacks that could be implemented in the BB84 protocol, but the QBC scheme
presented by Bennett doesn’t yield this attack [15]. In 2011, a quantum cryptographic method was introduced and applied to BC where Alice is required to send a quantum state at light speed over secure quantum channels in one of two or more directions [16]. In 2012, a practical bit commitment scheme is presented where the quantum state is supposed to be supplied by Bob and known to him but unknown to Alice. This gives unconditionally security against eavesdropper attacks [11]. In 2016, Unruh proposed a definition of computationally binding commitment schemes in the quantum setting called “collapse-binding” [17]. The definition is applied to string commitments, composes in parallel, and works with rewinding-based proofs.

In 2019, a simple QBC protocol was introduced to avoid the no-go proofs that are built using the Hughston–Jozsa–Wootters (HJW) theorem. In high-dimensional systems, a possible chaos effect in quantum steering can be displayed with some quantum states [18]. On the other hand, Ping showed that as long as time can be treated as a continuous variable then each infinite dimensional system in the unconditionally secure QBC protocol can be realized using a single photon. As a result, an experimental implementation of the QBC protocol is feasible under available technology [19].

In 2020, Mariana Gama et al. proposed a QBC protocol based on the entanglement aspects [8]. This protocol introduced the idea of string commitment. They suggested the use of physical unclonable functions to model random oracles, this protocol is not secure against eavesdropping attacks [8]. In 2021, Hao et al. proposed a QBC protocol that uses Bell states and demonstrates that the sender can successfully change her commitment without being detected by the recipient with a probability of $1-(1/2)n$, where $n$ is the number of rounds in executing the protocol. This means that the protocol is insecure because it cannot satisfy the binding condition [20].

This paper proposes a secured quantum commitment protocol that aims to commit two classical bits that are represented by a specific quantum state, where the two parties share one of the four maximally entangled two-qubit Bell states for satisfying the binding condition. The commitment and revealing phases are executed by using secure classical and quantum channels in addition to a two-qubit teleportation step to satisfy the concealing condition. The proposed protocol has been proved mathematically in all phases and simulated using Qiskit [21]. The simulated circuit combines all the phases of the proposed protocol. The commitment message 11 is simulated and discussed in the results and discussion section. The manuscript is organized as follows: section II introduces the basic assumptions of the proposed quantum two-bit commitment protocol, section III presents the details of the proposed framework and the mathematical model as well, section IV summarizes the results of this work as well as the implementation of the proposed protocol, and finally, the main conclusion of this work is reported.

II. MAIN METHODS
In order to make the work presented here self-contained, we introduce the main basic mathematical tools used for developing the proposed protocol. Two-qubit teleportation, diffusion Operator, and Grover algorithms are the main highlights of these tools.

A. PARTIAL DIFFUSION OPERATOR $D_p$
The Grover operator is used in search algorithms and in addition to multiple applications [22]. It performs the inversion about the mean. The diagonal representation of $G$ on an $n$-qubit system has the following form

$$G = W^\otimes n (|0\rangle \langle 0| - I) W^\otimes n.$$  \hspace{1cm} (1)

where $W$ represents the Walsh Hadamard gate, the vector $|0\rangle$ is of length $2^{n+1}$, and $I_n$ is the identity matrix [23]. Fig.1 presents the quantum circuit of the Grover’s operator for 2-qubit system.

Hiding quantum states from a superposition is used as a tool for increasing the security of data transmission through channels. It can be accomplished by using the partial diffusion operator, $D_p$ which has the following representation

$$D_p = (W^\otimes n \otimes I)(|0\rangle \langle 0| - I)(W^\otimes n \otimes I).$$  \hspace{1cm} (2)

It performs the inversion about the mean on the subspace of the system that is entangled with the third qubit in state $|0\rangle$ and performs a phase shift of $-1$ on the other subspace of the system that is entangled with the third qubit in state $|1\rangle$. The third qubit is an extra qubit that the sub-spaces are entangled with to distinguish between the states to be hidden and the ones to be selected. The oracle $U_f$ is an operator that evolves to be true for the target states [24]. The two-states selection is obtained using the operator $U_f$ in order to select the states that Alice chooses to be hidden where it satisfies the property that

$$U_f|x, 0\rangle \rightarrow |x, f(x)\rangle.$$  \hspace{1cm} (3)

In order to restore the states that were hidden using the partial diffusion operator, the Grover’s quantum operator $G$ is applied once [25]. Fig. 2 presents the implementation circuit of the partial diffusion operator including the performing of the phase shift followed by applying the inversion about the mean.

B. TWO-QUBIT TELEPORTATION
Teleportation was proposed by Bennet in 1993 [26]. Quantum teleportation is the transmission of quantum information.
between two distinct parties from one location to another with the help of a classical channel and previously shared quantum entanglement between distant laboratories [26]. Two-qubit teleportation can be performed using the probabilistic quantum teleportation that can be formulated as an unambiguous state discrimination problem and derives exact optimal Positive Operator Valued Measure POVM operators for maximizing the probability of unambiguous discrimination. Fig.3 illustrates the description of this teleportation protocol where Alice has three qubits, two of them are represented by the two-qubit state that Alice intends to teleport to Bob while the third is entangled with Bob in a GHZ state. A classical communication channel between the two parties is also used in the teleportation scheme.

According to [27], the teleportation of a two-qubit entangled state can be achieved using a GHZ state as a quantum channel probabilistically. Assume that Alice intends to teleport the two qubit entangled state

$$|\psi\rangle = \gamma |01\rangle + \delta |10\rangle,$$

where $\gamma$ and $\delta$ are normalized complex numbers. In this case, Alice and Bob share one non-maximally entangled GHZ state, which is

$$|\text{GHZ}\rangle = a|010\rangle + b|101\rangle,$$

where $a$ and $b$ are real numbers that satisfy $|a|^2 + |b|^2 = 1$ such that $|a| \geq |b|$ where the total success probability of the teleportation equals to $2|b|^2$ and reaches 1 when $|b| = \frac{1}{\sqrt{2}}$.

The entanglement is used as a quantum channel, through which Alice transmits a two-qubit entangled state to Bob. The combined five-qubit subsystem state can be expressed as follows

$$|\phi_{\text{sys}}\rangle = |\psi\rangle_{12} \otimes |\text{GHZ}\rangle_{345}. \quad (4)$$

The above equation can be expanded and rewritten as

$$\begin{align*}
\langle \text{GHZ}\rangle_{345} & = \frac{1}{2} (|b\rangle|011\rangle + |a\rangle|100\rangle)_{123} \otimes (|\gamma\rangle|01\rangle + |\delta\rangle|10\rangle)_{45}
+ \frac{1}{2} (|b\rangle|011\rangle - |a\rangle|100\rangle)_{123} \otimes (|\gamma\rangle|01\rangle - |\delta\rangle|10\rangle)_{45}
+ \frac{1}{2} (|a\rangle|010\rangle + |b\rangle|101\rangle)_{123} \otimes (|\gamma\rangle|10\rangle + |\delta\rangle|01\rangle)_{45}
+ \frac{1}{2} (|a\rangle|010\rangle - |b\rangle|101\rangle)_{123} \otimes (|\gamma\rangle|10\rangle - |\delta\rangle|01\rangle)_{45}. \quad (5)
\end{align*}$$

A joint measurement is executed on the three qubits possessed by Alice, so that the state on Bob’s two qubits would collapse into one of the four possible states. Consequently, the exact optimal POVM operator is derived to maximize the success probability [27].

Fig.4 describes the quantum circuit for the two qubit teleportation scheme. The sender specifies POVM to discriminate the state that comprises measurement operators $E_i$, where

$$1 \leq i \leq 4 \text{ and } \sum_{i=1}^{4} E_i = I.$$  

The resultant states are linearly independent and each $E_i$ corresponds to the detection of the state $|\phi_i\rangle$ where $|\phi_i\rangle$ are the reciprocal state associated with $|\phi_i\rangle$, and $p_i$ is the corresponding probability where the correct recognition of the quantum states on the first three qubits will successfully lead to the state on qubits 4 and 5.

Fig.5 illustrates the four discrimination cases of the POVM. The exact POVM contains the coefficients of the quantum channel to discriminate the state, on the other hand, Bob needs only to make a unitary operation consists of specific Pauli matrices, and so the original state can be recovered through the operation

$$T = (X^{m_1} Z^{m_2})_4 \otimes (X^{m_1})_5,$$
where $T$ represents the operation that is applied by Bob on the fourth and fifth qubits to reconstruct the original state. The symbols $m_1$ and $m_2$ represent the classical bit string which denotes the measurement outcomes of $E_i$

$E_1 \rightarrow 00$, $E_2 \rightarrow 01$, $E_3 \rightarrow 10$, and $E_4 \rightarrow 11$

and finally, $X$ and $Z$ are the used Pauli matrices. The gate $G_{4,5}^{[0,1]}$ represents the Pauli matrix that is used where the superscript has values 0 or 1 to denote whether the quantum gate will be applied to the qubit or not respectively.

The $T$ operation is applied on the subsystem:

$$\frac{1}{2}(b|011⟩ + a|100⟩)_{123} \otimes (γ|01⟩ + δ|10⟩)_{45}$$

as follows:

$$T = (X^0Z^0)_{4} \otimes (X^0)_{5},$$

$$X^0_4(γ|01⟩ + δ|10⟩) = (γ|01⟩ + δ|10⟩),$$

$$Z^0_4(γ|01⟩ + δ|10⟩) = (γ|01⟩ + δ|10⟩)_{45},$$

thus the final effect of the $T$ operator will be

$$T[(γ|01⟩ + δ|10⟩)_{45}] = (γ|01⟩ + δ|10⟩)_{45}. \quad (6)$$

The same analysis can be carried out for the rest of the cases as follows: when the measurement outcome $E_2 = 01$, the effect of $T$ will be on the subsystem

$$\frac{1}{2}(b|011⟩ - a|100⟩)_{123} \otimes (γ|01⟩ - δ|10⟩)_{45},$$

$$T = (X^0Z^0)_{4} \otimes (X^0)_{5},$$

$$T[(γ|01⟩ - δ|10⟩)_{45}] = (γ|01⟩ + δ|10⟩)_{45}. \quad (7)$$

When the measurement outcome $E_3 = 10$, the effect of $T$ will be on the subsystem

$$\frac{1}{2}(a|010⟩ + b|101⟩)_{123} \otimes (γ|10⟩ + δ|01⟩)_{45},$$

$$T = (X^1Z^0)_{4} \otimes (X^1)_{5},$$

$$T[(γ|10⟩ + δ|01⟩)_{45}] = (γ|01⟩ + δ|10⟩)_{45}. \quad (8)$$

Finally, when the measurement outcome $E_4 = 11$, the effect of $T$ will be on the subsystem

$$\frac{1}{2}(a|010⟩ - b|101⟩)_{123} \otimes (γ|10⟩ - δ|01⟩)_{45},$$

$$T = (X^1Z^1)_{4} \otimes (X^1)_{5},$$

$$T[(γ|10⟩ - δ|01⟩)_{45}] = (γ|01⟩ + δ|10⟩)_{45}. \quad (9)$$

By analyzing (6), (7), (8), and (9), it is obvious that Bob is always getting the exact state of Alice

$$(γ|01⟩ + δ|10⟩),$$

and this proves that the teleportation of the two-qubit state is achieved successfully.

III. THEORETICAL WORK

The proposed framework of the quantum two-bit commitment (Q2BC) is introduced in this section. The main phases are the Commitment phase and the Revealing phase which are denoted by the operators $C$ and $R$ respectively. The two-qubit teleportation $T_E$ is an essential step performed in the commitment phase.
A. THE PROTOCOL’s STRUCTURE
The protocol consists of two main steps namely commitment and revealing where the binding is performed during these two steps. The protocol uses two different channels to send quantum and classical data besides using two pre-defined two-qubit decoding unitary operator \( D_{AB} \) that is used before the measurements. The sender uses the classical channel to send the information regarding the necessary unitary transformations, while the quantum channel is used to communicate the teleportation part.

The proposed protocol performs a quantum commitment of two classical bits 00, 01, 10, or 11 depending on the sender’s choice. The commitment phase starts from Alice by preparing the commitment message and representing it by two qubits, followed by the two-qubit teleportation between Alice and Bob. In parallel, Alice and Bob share one of the Bell states in order to achieve the binding condition which is crucial to enable Bob ensuring that Alice hasn’t changed the committed message. Then, Alice applies a one qubit unitary transformation \( U_{A2} \) that is suitable for her choice of the commitment value, then Bob applies a secured unitary transformation \( U_B \) on the shared Bell state that can be chosen randomly in order to ensure that Alice will not perform any other transformations until reaching the revealing phase.

Alice applies the \( D_P \) operator for hiding the initialized quantum states within the superposition as an extra security layer [25]. After that, Alice applies the unitary operator \( U_{A1} \) which is chosen randomly to achieve the concealing condition of the protocol. At this moment, the state is ready to be teleported using a GHZ configuration as described in Section II.

In the revealing phase, Alice sends - over the classical channel - the quantum operators to decode the committed message to Bob. As shown in fig.6, Bob applies the received operators \( U_{A1}^\dagger \) and \( G \) followed by the decoding operators \( D_{AB_1} \), then performs a measurement on his qubits to get the committed message. The resulting value from the binding phase is compared with the Bob’s measurements. If the two outcomes are equivalent, then this proves the binding condition and consequently the commitment message is accepted. Otherwise, the commitment message will be rejected. The following subsections will discuss in details the main steps of the protocol.

B. THE COMMITMENT PHASE \( C \)
According to the proposed framework, the quantum system is initialized in the ground state as

\[ |\Psi_{sys}\rangle = |0\rangle^\otimes n \text{where } n = 7 \]

denotes the number of qubits. The operator \( C \) denotes the commitment phase and can be defined as in the following equation

\[
C = (H^\otimes 3 \otimes I) (CX_{(5,6)} \otimes I) (U_{A2} \otimes I) \\
\times (U_{B} \otimes I) (U_{f} \otimes I) (D_{P} \otimes I) \\
\times (U_{A1} \otimes I) (T_{E} \otimes I).
\]

As shown in fig.7, the resulting state \( |\Psi'\rangle = C|\Psi_{sys}\rangle \) is prepared by a superposition on Alice’s first two qubits and a Bell state between Alice and Bob’s last qubits followed by applying the unitary operator \( U_{A1} \) as stated in table. 2 and the randomly chosen unitary operator \( U_B \). Hence, Alice’s first two qubits that contain the committed message can be transformed into an ambiguous state using the selection effect of the quantum operator \( U_{f} \) as illustrated in (3) and the hiding
TABLE 1. Decoding unitary operators $D_{AB1}$.

| Commitment value | Corresponding $D_{AB1}$       |
|-------------------|-------------------------------|
| 00                | $X_0, Cx_{1,0}, Cx_{0,1}, H_0$ |
| 01                | $X_1, Cx_{1,0}, Cx_{0,1}, H_0$ |
| 10                | $X_0, Z_1, Cx_{1,0}, Cx_{0,1}, H_0$ |
| 11                | $X_1, Cx_{1,0}, Z_0, Cx_{0,1}, H_0$ |

FIGURE 7. The commitment phase $C$ of the Q2BC protocol. The two classical bits are represented by a two qubit state where Alice applies quantum transformations and then a two qubit teleportation is performed to Bob. In parallel, Alice and Bob share a Bell state to satisfy the binding condition.

The effect of the $D_p$ operator as illustrated in (2) on Alice’s first three qubits as previously mentioned in Section II. Then, the two qubit teleportation operator $T_E$ is applied between Alice’s first three qubits and Bob’s first two qubits. The requirement for having a binding condition is partially met and in the revealing phase it will be fulfilled.

C. TWO QUBIT TELEPORTATION $T_E$

In the proposed Q2BC protocol, the teleportation of two-qubit state is a fundamental step during the commitment phase and it is achieved by sharing one nonmaximally entangled GHZ state between the committer and the receiver. The entanglement is used as quantum channel, through which Alice intends to transmit the two-qubit entangled state

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

to Bob.

The teleportation scheme assumes that the information of the quantum channel is known by the sender but not the receiver, this means that the sender has a full knowledge of the coefficients of the quantum channel. The effect of operator $T_E$ on state $|\psi\rangle_{sys}$ is described by the following equation

$$T_E|\psi\rangle_{sys} = |\psi\rangle_{tele},$$

where $|\psi\rangle_{tele}$ represents the qubit state resulted from the teleportation scheme and can be expressed as

$$|\psi_{tele}\rangle = \gamma|01\rangle + \delta|10\rangle,$$

where $\gamma$ and $\delta$ are normalized complex numbers. The operator $T_E$ is described by the following equation

$$T_E = T(|\psi\rangle_{sys} \otimes |GHZ\rangle_{345}),$$

where $T$ is calculated by (6). The analysis of (13) is illustrated in (5). The proof of the two qubit teleportation scheme for the four discrimination cases is presented in Section II.

D. REVEALING PHASE $R$

The teleported state $\psi_{tele}$ can not be decoded - and hence the concealing condition is met - until Alice sends to Bob over the classical channel the following quantum operators denoted by $U_{A1}^\dagger$, $G$ and $D_{AB1}$, where the revealing phase can be represented by the following equation

$$R = U_{A1}^\dagger G D_{AB1}.$$

As shown in fig. 6, Bob can decode the message and perform the measurements. To ensure the success of the protocol and to fulfill the binding condition, both Alice and Bob applies the predetermined decoding two qubit unitary transformation $D_{AB1}$. If the resultant outcome from Bob’s measurement in the revealing phase is identical to the last two qubits of Alice and Bob, then the binding condition is met and the protocol has succeeded.

The revealing phase is executed when Alice sends the unitary transform $U_{A1}$, the Grover quantum operator $G$, and the decoding unitary operators $D_{AB}$, to Bob who applies the $U_{A1}^\dagger$ followed by the quantum operator $G$ to substitute the amplitudes of the existing states by the amplitudes of the hidden ones. The result of applying $G$ only once is the apparition of the hidden states and hiding the other quantum states [24]. Finally, the decoding unitary operators $D_{AB}$, are prepared by Alice for each commitment value, and through the shared classical channel, Alice sends the corresponding decoding unitary operators to Bob to restore the commitment classical two bits. Thus, the result of the revealing phase represents the two classical bits that Alice has committed to Bob. Table 1 illustrates the different decoding unitary operators depending on the value of the commitment value where Alice prepares and sends the decoding operators to Bob who applies them during the revealing phase.

IV. RESULTS AND DISCUSSION

The usage of Q2BC can be explored in a straightforward manner by analyzing each step of the protocol as shown in fig. 6. By setting the classical message to be 11, the commitment operator in (10) will evolve the state into a secured and robust one. As shown in fig. 6, Alice controls 4 qubits, while Bob controls the rest where the depth of the simulation circuit is 42. The initial state of the system is

$$|\Psi_{sys}\rangle = |0\rangle^\otimes 7.$$  

Firstly, applying two Hadamard gates on the first and the second qubits will result in

$$(H^\otimes 2 \otimes I)|\Psi_{sys}\rangle = \frac{1}{2}(|0000000\rangle + |0100000\rangle + |1000000\rangle + |1100000\rangle).$$

In parallel, a shared Bell state $|\Phi\rangle^+$ on a subsystem of $|\Psi_{sys}\rangle$ is prepared between Alice and Bob; specifically on the fifth volume.
FIGURE 8. Comparing the measurement values of the fourth and fifth qubits with the measurement values of the sixth and fifth qubits. The Q2BC protocol is successfully satisfied when the measurement values of the commitment message are equivalent to the measurement values that are resulted from the binding step.

TABLE 2. Secured unitary operators $U_{A2}$ by Alice.

| Commitment value | Corresponding $U_{A2}$ |
|------------------|------------------------|
| 00               | $I$                    |
| 01               | $X$                    |
| 10               | $Z$                    |
| 11               | $XZ$                   |

and the sixth qubits. So, the evolved state

$$|\Psi_{sys}'\rangle = \frac{1}{2\sqrt{2}} (|00000000\rangle + |00000011\rangle + |01000000\rangle + |01000011\rangle + |10000000\rangle + |10000011\rangle + |11000000\rangle + |11000011\rangle).$$

Alice then applies a unitary transformation $U_{A2}$ depending on her choice of the commitment message as illustrated in table 2. In this case, Alice performs a bit-flip gate followed by a phase-flip gate. Hence, $|\Psi_{sys}'\rangle$ will be transformed into

$$\frac{1}{2\sqrt{2}} (-|0000010\rangle + |0000001\rangle - |0100010\rangle + |0100001\rangle + |1000100\rangle + |1000011\rangle + |1100010\rangle + |1100001\rangle).$$

After that, Bob performs a unitary transformation $U_B$ that is not known to Alice, in order to protect the shared state from further modifications by Alice herself. Bob performs an $X$ gate as follows

$$(\mathbb{I} \otimes X_B)|\Psi_{sys}'\rangle$$

where 6 denotes the index of the qubit, and thus the system will be

$$|\Psi_{sys}''\rangle = \frac{1}{2\sqrt{2}} (-|0000011\rangle + |0000000\rangle - |0100011\rangle + |0100000\rangle - |1000111\rangle + |1000100\rangle - |1100011\rangle + |1100000\rangle).$$

For the selected secret message 11, the hidden states are $|10\rangle$ and $|11\rangle$ and the states to be selected are $|01\rangle$ and $|00\rangle$. Thus, the effect of the quantum operator $U_f$ on $|\Psi_{sys}''\rangle$ is

$$|\Psi_{sys}'''\rangle = \frac{1}{2\sqrt{2}} (-|0010011\rangle + |0010000\rangle - |0110011\rangle + |0110000\rangle - |1000011\rangle + |1000000\rangle - |1100011\rangle + |1100000\rangle).$$

From (2), the effect of the Partial diffusion operator on (15) will be

$$|\Psi_{sys}^{Diff}\rangle = \mathcal{D}_P|\Psi_{sys}'''\rangle$$

$$= \frac{1}{2} (|0010011\rangle - |0010000\rangle + |0110011\rangle - |0110000\rangle).$$
Alice applies a two-qubit unitary operator $U_A$, on the first two-qubits followed by applying a bit-flip gate on the second qubit. Hence,

$$|\psi_{sys}\rangle_{diff} = \frac{1}{2}(|01100111⟩ - |01100000⟩ + |10100111⟩ - |10100000⟩).$$

Afterwards, the two-qubit teleportation operator $T_C$ is applied as illustrated in Section II, where the two qubit state

$$|\psi⟩^+ = \frac{1}{\sqrt{2}}(|01⟩ + |10⟩)$$

is teleported from Alice to Bob. Eventually, the application of the operator $C$ on the initial state $|\psi_{sys}\rangle$ will result in

$$|\psi_{comm}\rangle = \frac{1}{4}(|10010000⟩ + |01010000⟩ + |01111000⟩ + |10001000⟩ + |01010100⟩ + |01101000⟩ + |01010111⟩ + |01101111⟩ + |10001111⟩ + |01001111⟩ + |01011011⟩ + |01011111⟩).$$

The same analytical analysis as described for the commitment phase can be performed for the revealing step. The effect of the revealing operator which is described in (14) on $|\psi_{comm}\rangle$ is

$$|\psi_{rev}\rangle = \mathfrak{R}|\psi_{comm}\rangle = \frac{1}{4}(|10011000⟩ + |01011000⟩ + |01111000⟩ + |10001000⟩ + |01011011⟩ + |01101111⟩ + |10001111⟩ + |01001111⟩ + |01011111⟩ + |01101111⟩ + |10110000⟩ + |10001000⟩ + |10110100⟩ + |10011011⟩ + |01111111⟩ + |01011111⟩ + |01011111⟩ + |01111111⟩).$$

The binding condition can be satisfied by applying a previously agreed unitary $D_{AB_2}$ on $|\psi_{rev}\rangle$. Following the same context of the classical message of 11, the $D_{AB_2}$ consists of two gates; $C_{X_{5,6}}$ and $H_5$ where the 5 and 6 denote the qubits’ indices. The final state of the system after applying the binding operators

$$|\psi_{sys}\rangle_{bind} = (C_{X_{5,6}}H_5 \otimes I)|\psi_{sys}\rangle_{rev} = \frac{1}{2}(|10011111⟩ + |01011111⟩ + |10111111⟩ + |01111111⟩).$$

By performing a standard measurement on the last 4 qubits, we can compare the output strings to check the validity of the protocol. The analysis and the simulation indicate that the measurement values of the qubits that represent the commitment message are equivalent to the measurement values of the qubits that satisfy the binding condition. Figs. 8a, 8b, 8c, and 8d show the four cases of the classical message and that the output string is identical and matches the desired classical message.

Compared with the protocol presented by Gama et al. [8] who performed only one bit at a time from the committed string, our protocol performed a commitment of two bits at a time. Furthermore, adding an authenticated channel is used in [8] to prevent man-in-the-middle attacks whereas our protocol executed the partial diffusion operator for hiding selected states from the superposition as an extra security level against eavesdropping attacks.

In contrast to the protocol presented by Hao et al. [20] who proved the insecurity of the binding condition in the cryptanalysis strategy that uses Bell state entanglement in its technical side, our protocol successfully proved the binding property using a shared Bell state between the two parties in parallel to the commitment phase.

One of the advantages of this approach is that both the binding and concealing conditions have been mathematically proved. Furthermore, the analysis of the proposed protocol shows that Alice can’t choose the unitary operator $U_A$, randomly. The main concern regarding the proposed protocol is that the failure of the teleportation step is not tolerable and this may affect the commitment protocol. This might be mitigated using more advanced schemes [28].

**V. CONCLUSION**

This paper proposed a general secure framework for the Q2BC. The achieved secured commitment protocol consists of commitment and revealing phases. The binding and concealing conditions have been proved. The simulation results showed the potential in the proposed protocol. The different security layers implied by the discussed operators managed to make it more robust against attackers. The protocol doesn’t allow any of the two parties to cheat. The aforementioned limitations of the protocol can be addressed in a future work. In addition to that, the simulation can include a simulated noisy environment to check for the validity at different noise levels.

**ACKNOWLEDGMENT**

The authors would like to thank Kareem H. El-Safty from Wigner Research Centre for Physics, Budapest, Hungary, for his valuable insights and comments.

**REFERENCES**

[1] K. Bharti, A. Cervera-Lierta, T. H. Kyaw, T. Haug, S. Alperin-Lea, A. Anand, M. Degroote, H. Heinonen, J. S. Kottmann, T. Menke, W.-K. Mok, S. Sim, L.-C. Kwek, and A. Aspuru-Guzik, “Noisy intermediate-scale quantum (NISQ) algorithms,” *Rev. Mod. Phys.*, vol. 94, no. 1, 2022, Art. no. 015004, doi: 10.1103/RevModPhys.94.015004.

[2] H. Abulkasim, A. Farouk, S. Hamad, A. Mashatan, and S. Ghose, “Secure dynamic multiparty quantum private comparison,” *Sci. Rep.*, vol. 9, no. 1, p. 17818, Nov. 2019.

[3] A. M. El-Mahalawy and K. H. El-Safty, “Classical and quantum regression analysis for the optoelectronic performance of NTCDAt/p-Si UV photodiode,” *Optik*, vol. 246, Nov. 2021, Art. no. 167793.

[4] Z. Tabi, K. H. El-Safty, Z. Kallus, P. Haga, T. Kozsik, A. Glos, and Z. Zimboras, “Quantum optimization for the graph coloring problem with space-efficient embedding,” in Proc. *IEEE Int. Conf. Quantum Comput. Eng. (QCE)*, Oct. 2020, pp. 56–62.
[5] Y. Cai, Z. Luo, and Y. Yang, “Rational multi-secret sharing scheme based on bit commitment protocol,” J. Netw., vol. 7, no. 4, Apr. 2012.

[6] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, 10th ed., Cambridge, U.K.: Cambridge Univ. Press, 2011.

[7] M. Blum, “Coin flipping by telephone a protocol for solving impossible problems,” ACM SIGACT News, vol. 15, no. 1, pp. 23–27, Jan. 1983.

[8] M. Gama, P. Mateus, and A. Souto, “A private quantum bit string commitment,” Entropy, vol. 22, no. 3, p. 272, Feb. 2020.

[9] L. Magnin, F. Magniez, A. Leverrier, and N. J. Cerf, “Strong no-go theorem for Gaussian quantum bit commitment,” Phys. Rev. A, Gen. Phys., vol. 81, no. 1, Jan. 2010, Art. no. 010302.

[10] A. Kent, “Unconditionally secure bit commitment,” Phys. Rev. Lett., vol. 83, no. 7, pp. 1447–1450, Aug. 1999.

[11] A. Kent, “Unconditionally secure bit commitment by transmitting measurement outcomes,” Phys. Rev. Lett., vol. 109, no. 13, Sep. 2012.

[12] D. A. Almubayedh, G. Alazman, M. Alkhalis, M. Alabdali, N. Nagy, M. Nagy, A. E. Tatar, M. Alfosail, A. Rahman, and N. AlMubairik, “Quantum bit commitment on IBM QX.” Quantum Inf. Process., vol. 19, no. 2, pp. 1–27, Feb. 2020.

[13] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” Theor. Comput. Sci., vol. 560, pp. 7–11, Dec. 2014.

[14] H.-L. Yin and Z.-B. Chen, “Secure BB84-type quantum key distribution with a simple phase error formula,” Opt. Lett., vol. 45, no. 7, p. 1627, Mar. 2020, doi: 10.1364/OL.387877.

[15] G. Brassard and C. Crépeau, “Quantum bit commitment and coin tossing protocols,” in Advances in Cryptology (CRYPTO), A. J. Menezes and S. A. Vanstone, Eds. Berlin, Germany: Springer, 1991, pp. 49–61.

[16] A. Kent, “Unconditionally secure bit commitment with flying qudits,” New J. Phys., vol. 13, no. 11, Nov. 2011, Art. no. 113015.

[17] D. Unruh, “Computationally binding quantum commitments,” in Proc. 35th Annu. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT), vol. 9066, Berlin, Germany: Springer-Verlag, 2016, pp. 497–527.

[18] G. Ping He, “Unconditionally secure quantum bit commitment based on the uncertainty principle,” Proc. Roy. Soc. A, Math., Phys. Eng. Sci., vol. 475, no. 2222, Feb. 2019, Art. no. 20180543.

[19] G. P. He, “An optical implementation of quantum bit commitment using infinite-dimensional systems,” 2019, arXiv:1909.09865.

[20] H. Cao, W. Ma, L. Lü, G. Liu, X. Liu, and W. Sun, “Crypanalysis and improvement of ‘Game theoretic security of quantum bit commitment,’” Inf. Sci., vol. 543, pp. 106–111, Jan. 2021.

[21] H. Abraham, Adoufifi, R. Agarwal, I. Y. Akhulwaya, G. Aleksandrowicz, and T. A. Cepalkovskis, “Qiskit: An open-source framework for quantum computing,” IBM, Endicott, NY, USA, Tech. Rep., Mar. 2019.

[22] C.-H. Cho, C.-Y. Chen, K.-C. Chen, T.-W. Huang, M.-C. Hsu, N.-P. Cao, B. Zeng, S.-G. Tan, and C.-R. Chang, “Quantum computation: Algorithms and applications,” Chin. J. Phys., vol. 72, pp. 248–269, 2021.

[23] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in Proc. 28th Annu. ACM Symp. Theory Comput. (STOC), New York, NY, USA, 1996, p. 212.

[24] A. Younes, “Enhancing the security of quantum communication by hiding the message in a superposition,” Inf. Sci., vol. 181, no. 2, pp. 329–334, Jan. 2011.

[25] A. Younes, J. Rowe, and J. Miller, “Enhanced quantum searching via entanglement and partial diffusion,” Phys. D: Nonlinear Phenomena, vol. 237, no. 8, pp. 1074–1078, Jun. 2008.

[26] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels,” Phys. Rev. Lett., vol. 70, no. 13, pp. 1895–1899, Mar. 1993.

[27] K. Wang, X.-T. Yu, and Z.-C. Zhang, “Teleportation of two-qubit entangled state via non-maximally entangled GHZ state,” Proc. Comput. Sci., vol. 131, pp. 1202–1208, Jan. 2018.

[28] X.-Z. Zhou, X.-T. Yu, and Z.-C. Zhang, “Multi-hop teleportation of an unknown qubit state based on W states,” Int. J. Theor. Phys., vol. 57, no. 4, pp. 981–993, Apr. 2018.

**AHMED YOUNES** received the Ph.D. degree from the University of Birmingham, U.K., in 2004. He is currently a Professor of computer science (quantum computing) with Alexandria University and an Honorary Research Fellow with the School of Computer Science, University of Birmingham. He is also the Founder and a Leader of the Alexandria Quantum Computing Group.