Quantum Information Processing (2026) 25:161
https://doi.org/10.1007/s11128-026-05175-4

A novel centralised e-payment protocol based on superdense coding

Zeynep Çelik[1] · **Hüseyin Bodur**[2]

Received: 1 February 2026 / Accepted: 10 April 2026

Abstract
The security and anonymity of e-payment transactions are paramount. In this study, we propose a centralised e-payment protocol based on superdense coding. By adopting quantum key establishment principles inspired by quantum key distribution (QKD) and combining them with superdense coding-based message transmission, symmetric key encryption, and two-particle entanglement, our quantum e-payment protocol utilises Bell states to reduce the complexity of quantum resources. The protocol is used for both key distribution and secure message transmission between the communicating parties. It is also resilient against quantum attacks and provides operational non-repudiation and immutability. Compared to previously proposed protocols, our protocol offers improved security while maintaining practical feasibility for real-world applications.

Keywords E-payment · Superdense coding · Quantum key distribution (QKD) · Quantum secure direct communication (QSDC) · Quantum e-payment system

1 Introduction

Today, innovations in e-commerce have enabled the ongoing development of electronic payment (e-payment) infrastructure, increasing the use of e-payments. E-payment transactions have gradually become part of daily life. Numerous protocols have been developed to ensure that e-payment transactions are conducted securely and efficiently. The security of these protocols is based on classical cryptography methods [1–8].

The security of classical cryptographic methods relies on various mathematical problems, such as integer factorisation and discrete logarithms. Solving these problems within practical timeframes is not considered feasible with current classical

✉ Hüseyin Bodur
huseyinbodur@duzce.edu.tr

Zeynep Çelik
zeynep215061@ogr.duzce.edu.tr

1 Institute of Graduate Studies, Düzce University, 81620 Konuralp, Düzce, Turkey

2 Department of Computer Engineering, Düzce University, 81620 Konuralp, Düzce, Turkey

Published online: 04 May 2026

computer technology, which is based on classical bits. Therefore, classical cryptographic methods currently provide security in many areas, including public services, military applications, healthcare, banking, e-commerce, and finance.

Although it is not considered possible to solve complex mathematical problems with classical computer technology, the existence of quantum computers and ongoing developments in quantum computing have the potential to undermine the reliability of these problems and the methods based on them [9, 10].

The existence of quantum computers, which are based on quantum bits (qubits), and the algorithms that can be used on these computers are compelling classical cryptographic methods and the fields in which they are used to change [11–13].

Quantum communication technologies have introduced new paradigms for secure information exchange. One of the most well-known approaches is QKD, which enables two parties to generate a shared secret key using the principles of quantum mechanics. In addition to QKD, another important paradigm is quantum secure direct communication (QSDC), which allows the direct transmission of secret messages through quantum channels without first generating a shared key.

Long and Liu proposed a theoretically efficient high-capacity quantum communication scheme based on Einstein–Podolsky–Rosen (EPR) entanglement and the superdense coding principle [14]. Deng et al. later introduced a two-step QSDC protocol in which channel security is first verified before transmitting the confidential message directly over the quantum channel [15]. Subsequent studies have explored practical implementations of QSDC. For example, Zhang et al. demonstrated QSDC using quantum memory to store entangled photon pairs and improve communication reliability [16]. Pan et al. provided a comprehensive survey of QSDC developments and discussed its potential role in future quantum internet (Qinternet) infrastructures [17]. Recent experimental progress has also demonstrated scalable and long-distance QSDC networks, such as a 15-user communication network proposed by Qi et al. [18] and a fully connected 300-km QSDC network demonstrated by Yang et al. [19].

In this study, a centralised quantum e-payment protocol is proposed. It is based on the fundamental laws of quantum mechanics to ensure the security of e-payment transactions. The protocol first establishes shared cryptographic keys between parties using quantum communication and subsequently uses the same quantum channel to securely transmit encrypted message segments, using quantum gates and the entanglement principle of qubits. In addition to key distribution, all message transmissions between the parties are also conducted via a quantum channel. This makes the protocol resilient against both quantum adversaries and classical cryptanalysis.

Our main contributions in this paper are summarised as follows:

1. To enhance security, we propose a centralised quantum payment protocol that employs techniques such as secret key encryption, pseudo-bit insertion, and either orderly or random data transmission.
2. The presented protocol provides anonymity, unforgeability, and undeniability and is resistant to CNOT, intercept-and-resend, inside one-way, and entangle-and-measure attacks.
3. Unlike decentralised quantum payment schemes, a centralised architecture enables regulatory compliance, dispute resolution, and commission handling, which are

mandatory in real-world payment systems. Therefore, the presented protocol is more suitable for real-world payment systems as it commissions transactions.
4. To the best of our knowledge, this is the first study integrating superdense coding with a centralised quantum e-payment architectures, combined with dynamic transmission ordering and pseudo-bit obfuscation.

2 Related works

Numerous studies on quantum computing and quantum communication have been reported in the literature. In one of these studies, Bennett and Brassard proposed the first QKD protocol. This protocol relies on transmitting key distribution information by encoding it in different polarisation directions of a photon [20]. In another study, Gou et al. proposed an e-payment protocol based on QKD, quantum proxy blind signature, and blockchain. The protocol uses three-qubit entangled states to minimise the complexity of quantum resources and employs blockchain to improve resilience and fairness [21]. In their study, Wen et al., unlike in their previous studies [22, 23], developed a protocol based on a one-time pad and quantum proxy blind signature for secure electronic payment transactions between two different banks. After the money transfer, the proxy signature is delegated to the merchant's bank [24].

Fatonah et al. conducted a literature review of e-payment systems in e-commerce. However, the review highlighted the need for further research on the importance of security in electronic payment systems and has a relatively narrow scope [25]. In another study, Li et al. presented a measurement-device-independent quantum e-payment protocol to eliminate side-channel attacks on detectors. The protocol includes single qubit, and Bell states, and utilises quantum public key encryption and blockchain to enhance security [26]. In their study, Li et al. proposed a twin-field quantum encryption protocol to enable eavesdropping detection and identity authentication. The protocol utilises single photons to minimise quantum resource complexity [27].

Wang et al. proposed a measurement-device-independent quantum secure digital payment protocol to eliminate side-channel attacks on detectors. Unlike [26], the protocol includes entangled photon pairs and the BB84 protocol, enabling secure data transmission without pre-shared keys [28]. In another study, Tiliwalidi et al. proposed a quantum proxy blind signature protocol based on six-qubit entangled states, supporting multi-bank payments. It also utilises a one-time pad to increase security [29]. In their study, Song et al. introduced a novel aspect for quantum computing's application in federated learning, especially in scenarios with limited quantum resources [30].

Zhang et al. proposed a third-party e-payment scheme based on a quantum group blind signature, a one-time pad, and QKD. The scheme is based on four-qubit states to ensure security [31]. In another study, Niu et al. proposed a quantum payment system based on a quantum signature and investigated an inter-bank quantum payment system [32]. In their study, Zhang et al. proposed a blockchain and quantum signature-based e-payment protocol. Similar to [29], the protocol uses six-qubit entangled states, and the purchase message is split into two parts to ensure blindness and increase security [33].

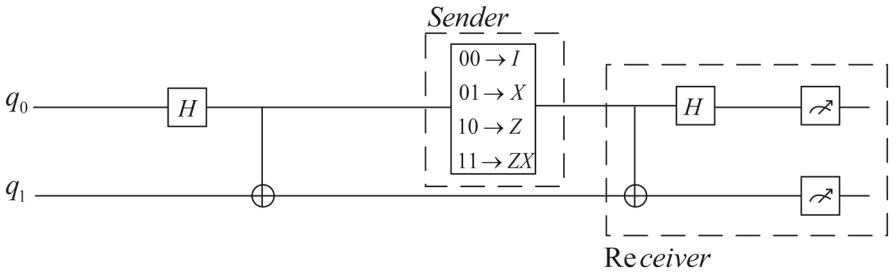

Fig. 1 Superdense coding gate operations

Gupta et al. proposed an electronic cash-based transaction scheme with quantum protocols. Unlike [21, 28, 29], and [33], the scheme does not require entanglement between parties [34]. In another study, Xie et al. proposed an inter-bank e-payment scheme using the entanglement properties of four-particle cluster states [35]. In their study, Yu et al. proposed a certificateless blind signcryption model based on lattice-based cryptography for an e-cash environment [36].

Qin et al. focused on the security of the communication process in the quantum private query protocol, which utilises QKD. They improved the original protocol and proposed a new version that uses the decoy state method to protect against multiphoton attacks [37]. In another study, Schiansky et al. implemented a quantum digital payment system that combines QKD and a quantum token. They demonstrated a payment application and presented its technical details and sample code [38].

Blockchain is a decentralised data management technology that removes the need for third-party approval of peer-to-peer network transactions [39]. This technology aims to perform verification and confirmation processes by eliminating the need for a central approval authority through consensus among network members [40]. Using blockchain for electronic payment transactions is an effective solution for data integrity and security. However, studies [21, 26, 27] and [33] indicate that using blockchain, which removes the role of a central approval authority, alongside centralised entities such as banks, leads to inconsistencies.

3 Superdense coding

It is a quantum communication protocol for sharing a classical bit sequence by transmitting a small number of qubits over a quantum channel between the sender and receiver. Although the idea was proposed earlier, it was formally published by Bennett and Wiesner in 1992 [41].

As shown in Figure 1, according to the superdense coding protocol, one of the entangled EPR pairs in Equation 1 must exist between the sender and the receiver before data transmission.

Table 1 Definitions of notations

Notations	Definitions
Id_A	Alice's identity
Id_B	Bob's identity
$Account_A$	Alice's bank account
$Account_B$	Bob's bank account
$Account_{OSP}$	The OSP's bank account
Key_{AOSP}	The shared secret key between Alice and the OSP
Key_{BOSP}	The shared secret key between Bob and the OSP
Key_{AB}	The shared secret key between Alice and $Bank_A$
Key_{OSPAB}	The shared secret key between the OSP and $Bank_A$

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad |\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$
$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \quad |\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{1}$$

According to quantum superdense coding, two classical bits can be transmitted using a single qubit [42]. This enables more classical information to be transmitted using fewer quantum resources. The main limitation of the protocol is that the sender transmits two classical bits of information by sending one qubit at a time to the receiver. If a classical bit sequence is shared via quantum superdense coding, it can serve as a key for encryption and decryption in a currently used encryption algorithm.

4 Proposed protocol

Although the protocol employs quantum principles for secure key establishment, the data transmission mechanisms described in Sections 4.1.1 and 4.1.2 are conceptually closer to quantum secure direct communication (QSDC). In the proposed architecture, superdense coding is used as the quantum transmission mechanism both for key establishment and encrypted message delivery. Therefore, the protocol is regarded as a hybrid scheme combining QKD-based key establishment with QSDC-like data transmission.

In this section, we present the protocol, which is divided into three phases: Initialisation Phase, Purchase Phase, and Payment Phase. In our protocol, there are three participants: Alice represents the customer, whereas Bob represents the merchant. The OSP is an Online Shopping Platform. Bank A is the bank of Alice. Bank B is the bank of Bob. Bank OSP is the bank of the OSP. All notations are defined in Table 1.

Alice, Bob, and the Online Shopping Platform (OSP) may have different banks. For the successful completion of the e-payment transaction, various key distribution operations must first be performed between the parties. In studies [24] and [26], key distribution was carried out using the BB84 protocol; in study [21], it was performed

using photons; and in studies [29, 31–33], and [35], the controlled quantum teleportation method was used. In the presented protocol, the superdense coding method is used for all data transmission, with data sent in two methods: orderly and random.

In the payment methods proposed in studies [21–38], the OSP, which is the intermediary platform and is referred to by different names, does not include commission or bank information. However, these platforms, which have an electronic payment system, conduct transactions between the buyer and the seller to collect the commission fee. Therefore, systems that do not include the $Bank_{OSP}$ and commission information in payment systems are not practical for daily use, even if they provide secure electronic payment. Including the intermediary platform's commission in the presented protocol makes it more useful for real-world applications.

In data transmission between parties, some of the transmitted data are not available to the recipient. For example, when Alice makes a purchase, she communicates with the OSP rather than directly with her own bank. Therefore, the message Alice sends to the OSP includes a section she must send to her own bank. In this case, the message must consist of several sub-parts. One part is data required by the OSP, while the other is data that Alice needs to send to her bank via the OSP. To ensure confidentiality and prevent the OSP from accessing the other part of the message, studies [21, 24, 29, 31–35], and [36] have used blind encryption. Study [26] used public key encryption, [27] used secret key encryption, and [28] used one-time pad encryption. In the proposed study, shared secret keys established between the parties during the initial phase are used. In this way, each party knows only the part of the message relevant to them.

4.1 Structure of the proposed protocol

This section discusses the methods used in our protocol.

4.1.1 Orderly binary send

In the orderly binary send method, two bits of data are transmitted sequentially from the sender to the receiver at each step. The message to be sent is first converted into binary format. The binary data are then transmitted in two groups sequentially. For the transmission of two bits of data at each step, the sender must perform the appropriate gate operation on the sender side in Figure 1. In the orderly binary send method, 'c' is set to 0 for the controlled Hadamard. This prevents the Hadamard gate from being applied to q_0 and q_1.

In $|\beta_{00}\rangle$, q_2 must pass through gate Id to send '00,' through gate X to send '01,' through gate Z to send '10,' and through gates Z and X, respectively, to send '11.'

As shown in Figure 3, on the sender side, the sender first prepares an EPR pair (q_2 and q_3). The sender then performs an XOR operation on the two data bits, q_0 and q_1, with q_2 and q_3, respectively, and uses the resulting values as exponents for the Z and X gates. In this way, the sender determines which gates to apply to q_2 and prepares the two particles, q_2 and q_3. On the receiver side, to receive the transmitted data, it is sufficient to apply the CNOT gate to q_2 and q_3, apply the Hadamard gate to q_2, and then measure.

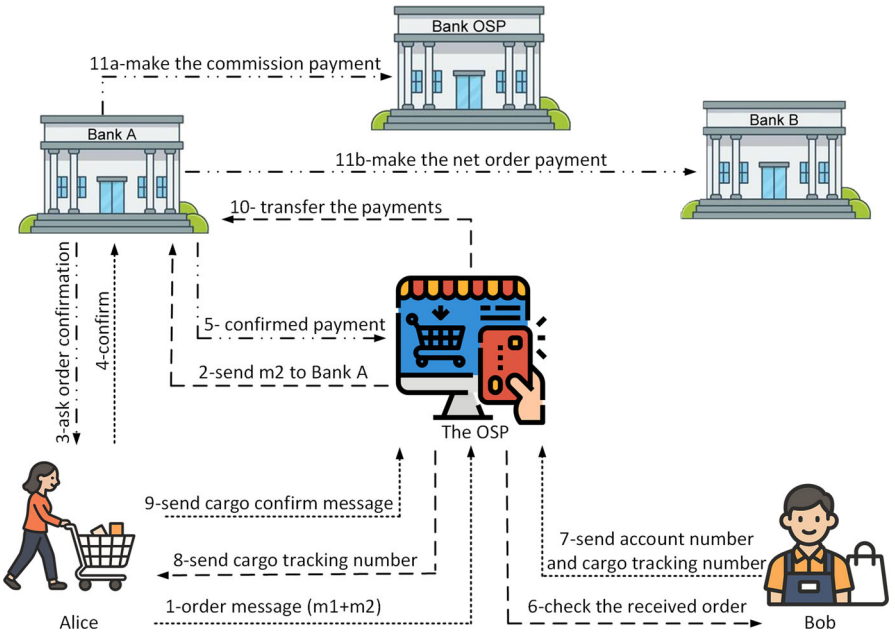

Fig. 2 The framework of the centralised e-payment protocol

After transmission, channel security is verified using the eavesdropping detection procedure described in Section 4.1.5.

4.1.2 Random binary send

The random binary send method increases uncertainty for the adversary by preventing reliable inference of message order and correlation patterns. Unlike orderly transmission, random transmission disrupts statistical analysis and replay-based correlation attacks, thereby reducing the adversary's success probability.

In the random binary send method, two random bits are generated at the sender's end. The message to be sent is first converted into binary format. The binary data are then divided into two sets. The randomly generated two bits are compared with the bits of the binary message. If two consecutive bits in the binary message match the randomly generated bits, the binary message is sent to the receiver. The index values of the two corresponding bits in the binary message are also recorded in a list. This process continues in a loop until the entire binary message has been sent. At the end of the loop, the list containing the index values corresponding to the binary bits must be sent to the receiver. This allows the receiver to arrange each two-bit segment according to its index value and reconstruct the binary message.

The random binary send method transmits two random bits from a different sequence of the binary message each time. This increases the security of the transmission medium against attacks. However, if the randomly generated two bits do not

match the binary bits in the original message, the method must be repeated until matching bits are generated. Therefore, as shown in Sect. 6, the random binary send method requires more executions than the orderly binary send method for transmitting a binary message.

In the random binary send method, c is set to 1 for the controlled Hadamard operation. This ensures randomness by applying Hadamard gates to q_0 and q_1.

In Figure 3, on the sender side, the sender first prepares an EPR pair (q_2 and q_3). The sender then prepares two particles, q_0 and q_1, applies Hadamard gates to both, and performs a measurement. This generates two random bits to be transmitted to the receiver. Next, the sender applies an XOR operation between q_0 and q_2, then applies a Z gate to the result, and applies an XOR operation between q_1 and q_3, followed by an X gate. This determines which gates are applied to the transmitted data.

On the receiver side, to retrieve the transmitted data, it is sufficient to apply a CNOT gate to q_2 and q_3, apply a Hadamard gate to q_2, and then perform a measurement.

After transmission, channel security is verified using the eavesdropping detection procedure described in Sect. 4.1.5.

4.1.3 Send with orderly or random

Algorithm 1 sendWithOrderlyOrRandom(binaryMessageData)

```
sendingType=random.randrange(0, 2)
if sendingType==0 then
    orderlyBinarySend(binaryMessageData)
else
    randomBinarySend(binaryMessageData)
end if
```

This method ensures that data transmission from the sender to the receiver occurs either in an ordered or a random manner. As shown in Algorithm 1, each time the method is invoked, and a random transmission mode is selected: A value of 0 initiates sequential data transfer, whereas a value of 1 results in random data transmission.

4.1.4 Add/Remove pseudo-bits

In the proposed protocol, pseudo-bits are inserted into the transmitted bit sequence to enhance security against eavesdropping attacks. These pseudo-bits do not carry meaningful information and are randomly positioned among the actual message bits. As an eavesdropper cannot distinguish pseudo-bits from real message bits, any interception attempt requires measuring all transmitted qubits. According to the principles of quantum mechanics, such measurements introduce disturbances in the quantum states. These disturbances can be detected by the legitimate parties during the verification stage. Therefore, pseudo-bits serve as decoy elements that increase uncertainty for an attacker and improve the protocol's resistance to interception and measurement attacks.

The Add pseudo-bits method inserts pseudo-bits into various parts of the binary message on the sender's side, thereby altering the data to be transmitted to the receiver. The Remove pseudo-bits method is designed to eliminate these pseudo-bits from the binary message at the receiver. In the Add pseudo-bits method, pseudo-bits can be inserted in three ways: after every two, four, or eight bits.

Suppose the message to be sent is 0001101100011011, and a pseudo-bit is appended after every two bits. Initially, the message is divided into binary pairs as follows: 00 01 10 11 00 01 10 11. Subsequently, for each pair, a randomly generated bit—either 0 or 1—is produced and appended to the end of the corresponding binary group: '00**1**01**0**10**0**11**1**00**0**01**0**10**1**111**1**.' In the Remove pseudo-bits method, the inserted pseudo-bits are removed based on the selected type, thereby recovering the original message.

As a result, an adversary attempting to intercept the transmission cannot determine which bits contain meaningful information. Any attempt to measure all transmitted qubits inevitably disturbs the quantum states, allowing the legitimate parties to detect the presence of an eavesdropper. However, these methods result in increased message size due to the added pseudo-bits and require more superdense coding operations.

4.1.5 Eavesdropping detection

To preserve the fundamental advantage of quantum communication, the proposed protocol incorporates an eavesdropping detection procedure after the transmission stage. During the communication process, a subset of the transmitted qubits is randomly selected as checking qubits. These qubits are not used for message reconstruction but serve as security verification samples.

After the receiver performs the quantum measurements, the sender reveals through the classical channel the encoding information corresponding to the selected checking qubits. The receiver compares the measurement outcomes with the expected values to estimate the quantum bit error rate (QBER) of the channel. Let N_c denote the number of checking qubits and N_e the number of mismatched measurement results. The error rate is calculated as

$$QBER = \frac{N_e}{N_c} \tag{2}$$

If the observed error rate exceeds a predefined error threshold e_{th}, the presence of a potential eavesdropper or excessive channel noise is assumed and the protocol is immediately aborted. Otherwise, the transmission is considered secure and the remaining qubits are used for the subsequent stages of the protocol.

This verification mechanism enables the legitimate parties to detect interception attempts, since any measurement performed by an eavesdropper inevitably disturbs the quantum states according to the principles of quantum mechanics. Consequently, the protocol retains the intrinsic capability of quantum communication systems to detect eavesdropping and ensure the integrity of the transmitted information.

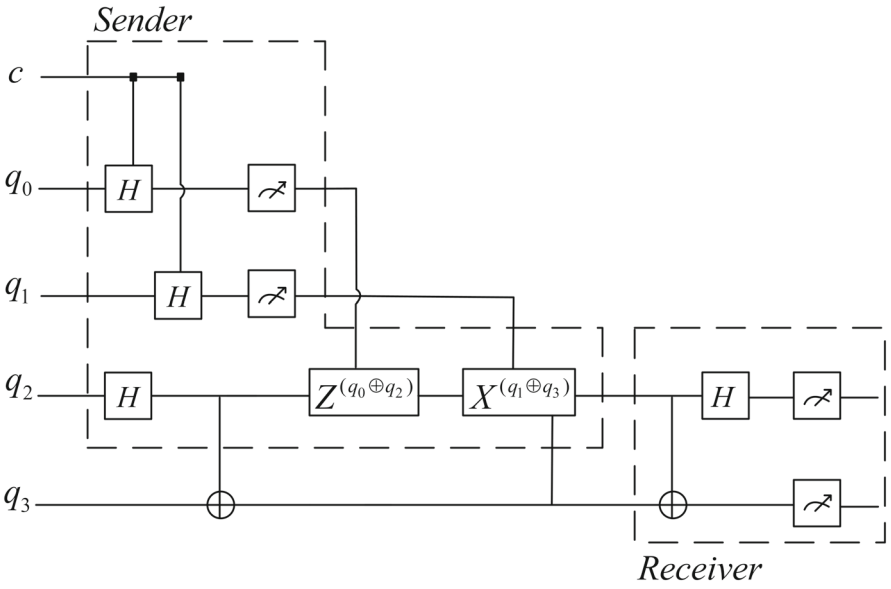

Fig. 3 The quantum gate operations of the proposed e-payment protocol

4.2 Phases

As shown in Figure 2, our protocol includes the following steps.

1. Alice sends an order message to the OSP, encrypted with the shared secret key Key_{AOSP}. The message consists of two parts: $order_{message} = m1_{Key_{AOSP}} + m2_{Key_{AB}}$ m1 contains Id_A, Id_B, the order number, information about the order she wants to buy, and the order date. m2 contains $Account_A$, the order information (gross order price, commission price calculated by the system during the order, and net order price).
2. The OSP decrypts message m1, which arrives encrypted with Key_{AOSP}. It obtains the order information, Id_A and Id_B. As it does not know Key_{AB}, it cannot access $Account_A$ or the order price. The OSP forwards the m2 message to $Bank_A$.
3. $Bank_A$ decrypts the m2 message with Key_{AB}. It checks the order price against $Account_A$. If the order price is eligible for Alice to pay, it sends her a confirmation message. This confirmation message includes a randomly generated one-time password (OTP).
4. Alice is expected to provide her approval within the timeframe set by her bank.
5. When Alice gives her approval, $Bank_A$ sends a confirmation message to the OSP, encrypted with Key_{OSPAB}. If Alice disapproves, $Bank_A$ sends a cancellation order message to the OSP.
6. Upon receiving the confirmation message, the OSP, knowing Id_B, uses Key_{BOSP} to send the order information to Bob.
7. Bob checks the order information. At this stage, Bob can cancel the order by sending a cancellation message to the OSP if he wishes. When the order is shipped,

he sends the cargo tracking number and $Account_B$ encrypted with $Key_B OSP$ to the OSP.

8. The OSP decrypts Bob's message using Key_{BOSP} and obtains a cargo tracking number and $Account_B$. The OSP then encrypts the cargo tracking number using Key_{AOSP} and sends it to Alice.
9. Alice decrypts the message from the OSP using Key_{AOSP} and obtains the cargo tracking number. Upon receiving the cargo, she encrypts a confirmation message using Key_{AOSP} and sends it back to The OSP. The confirmation message contains $Bank_A$'s OTP, which was sent to her.
10. Upon receiving the confirmation message, the OSP decrypts the message from Alice using Key_{AOSP} and obtains the OTP. Then, it encrypts Bob's account information $Account_B$, its own account information $Account_O SP$, and OTP using Key_{OSPAB} and sends them to $Bank_A$ to complete the payment process.
11. $Bank_A$ decrypts the encrypted message it receives from the OSP using Key_{OSPAB}. It compares the OTPs. If they match, it completes the payment process by sending the commission amount included in the m2 message received in Step 3 to $Account_{OSP}$ and the net order amount to $Account_B$.

4.2.1 Initialisation Phase

In our quantum centralised e-payment protocol, we assume that Alice, Bob, and the OSP are semi-honest. Alice's, Bob's, and Trent's banks are honest. Alice and Bob register with the OSP using their own identities. The OSP is initially considered trustworthy and honest. The OSP prepares Bell pairs, giving one half of each pair to Alice or Bob, while retaining the other half for itself. This enables the OSP to use these pairs when communicating with Alice or Bob. In the proposed centralised e-payment method, shared secret keys are used to encrypt all data transmissions between the parties. During registration, participants establish shared secret keys using AES-256, a symmetric encryption algorithm.

This process follows the fundamental principles of QKD, where quantum states are used to securely establish shared secret keys. However, unlike traditional QKD protocols such as BB84, the proposed protocol employs the superdense coding mechanism for transmitting key bits over the quantum channel. To obtain a shared secret key, one party first generates two bits of random data. This data is then processed through the relevant gates on the sender side (Figure 3), and the resulting entangled state is transmitted to the other party. On the receiver side, the other party applies CNOT and Hadamard gates to the received entanglement to recover the two-bit data. For a 256-bit AES key, this process, in which two bits are transmitted each time, is repeated 128 times. The 256-bit binary data obtained by both parties are converted into 32 bytes and used as the AES key for encryption and decryption operations.

4.2.2 Purchase Phase

Algorithm 2 presents the pseudo-code of the Purchase Phase of the proposed protocol.

Algorithm 2 Purchase phase

Step 1 - Alice:

$m1_{encrypted} = (Id_A + Id_B + orderNumber + details + datetime)_{Key_{AOSP}}$
$m2_{encrypted} = (Account_A + orderPrice + commission + netPrice)_{Key_{AB}}$
$order_{messageBits} = convertToBinary(m1_{encrypted} + m2_{encrypted})$
$sendWithOrderlyOrRandom(order_{messageBits}, OSP)$

Step 2 - The OSP:

$m1_{encrypted}, m2_{encrypted} = convertToString(order_{messageBinary})$
$m1 = m1_{encrypted_{Key_{AOSP}}}$
$m2_{encryptedBinary} = convertToBinary(m2_{encrypted})$
$sendWithOrderlyOrRandom(m2_{encryptedBinary}, Bank_A)$

Step 3 - $Bank_A$

$m2_{encrypted} = convertToString(m2_{encryptedBinary})$
$m2 = m2_{encrypted_{Key_{AB}}}$
$confirmMesssage_{encrypted} = (orderPrice + "confirm?" + OTP)_{Key_{AB}}$
$confirmMesssage_{encryptedBinary} = convertToBinary(confirmMesssage_{encrypted})$
$sendWithOrderlyOrRandom(confirmMesssage_{encryptedBinary}, Alice)$

Step 4 - Alice:

$confirmMesssage_{encrypted} = convertToString(confirmMesssage_{encryptedBinary})$
$orderPrice, "confirm?" + OTP = confirmMesssage_{encrypted_{Key_{AB}}}$
$orderConfirm_{encrypted} = "\text{I Confirm The Order}"_{Key_{AB}}$
$orderConfirm_{encryptedBinary} = convertToBinary(orderConfirm_{encrypted})$
$sendWithOrderlyOrRandom(orderConfirmencryptedBinary, Bank_A)$

Step 5 - $Bank_A$:

$orderConfirm_{encrypted} = convertToString(orderConfirm_{encryptedBinary})$
"I Confirm The Order"$= orderConfirm_{encrypted_{Key_{AB}}}$
$confirmMesssage2_{encrypted} = "AliceConfirmsTheOrder"_{Key_{OSPAB}}$
$confirmMesssage2_{encryptedBinary} = convertToBinary(confirmMesssage2_{encrypted})$
$sendWithOrderlyOrRandom(confirmMesssage2_{encryptedBinary}, OSP)$

4.2.3 Payment Phase

Algorithm 3 presents the pseudo-code of the Payment Phase of the proposed protocol.

5 Analysis and discussion

As shown in Table 2, classical cryptographic approaches enhanced with PQC primarily rely on computational hardness assumptions and therefore cannot provide information-theoretic security or intrinsic detection of active eavesdropping. In contrast, the presented protocol leverages fundamental principles of quantum mechanics, particularly entanglement and measurement disturbance, to achieve information-theoretic security and detect active interception attempts on the communication channel. Furthermore, the use of orderly and random binary transmission modes enables implicit

Algorithm 3 Payment phase

Step 1 - The OSP:

$m3_{encrypted} = (orderNumber + details + datetime)_{Key_{BOSP}}$
$m3_{encryptedBinary} = convertToBinary(m3_{encrypted})$
$sendWithOrderlyOrRandom(m3_{encryptedBinary}, Bob)$

Step 2 - Bob:

$m3_{encrypted} = convertToString(m3_{encryptedBinary})$
$m3 = m3_{encrypted_{Key_{BOSP}}}$
$CargoAndAccount_{B_{encrypted}} = (CargoTrackingNumber + Account_B)_{Key_{BOSP}}$
$CargoAndAccount_{B_{encryptedBinary}} = convertToBinary(CargoAndAccount_{B_{encrypted}})$
$sendWithOrderlyOrRandom(CargoAndAccount_{B_{encryptedBinary}}, OSP)$

Step 3 - The OSP:

$CargoAndAccount_{B_{encrypted}} = convertToString(CargoAndAccount_{B_{encryptedBinary}})$
$CargoTrackingNumber + Account_B = CargoAndAccount_{B_{encrypted_{Key_{BOSP}}}}$
$Cargo_{encryptedBinary} = convertToBinary(CargoTrackingNumber_{Key_{AOSP}})$
$sendWithOrderlyOrRandom(Cargo_{encryptedBinary}, Alice)$

Step 4 - Alice:

$Cargo_{encrypted} = convertToString(Cargo_{encryptedBinary})$
$CargoTrackingNumber = Cargo_{encrypted_{Key_{AOSP}}}$
$cargoConfirm_{encrypted} = \text{"(Cargo Confirm"} + OTP)_{Key_{AOSP}}$
$cargoConfirm_{encryptedBinary} = convertToBinary(cargoConfirm_{encrypted})$
$sendWithOrderlyOrRandom(cargoConfirm_{encryptedBinary}, OSP)$

Step 5 - The OSP:

$cargoConfirm_{encrypted} = convertToString(cargoConfirm_{encryptedBinary})$
$\text{"Cargo Confirm+}OTP\text{"} = cargoConfirm_{encrypted_{Key_{AOSP}}}$
$Accounts_{encrypted} = (Account_B + Account_{OSP} + OTP)_{Key_{OSPAB}}$
$Accounts_{encryptedBinary} = convertToBinary(Accounts_{encrypted})$
$sendWithOrderlyOrRandom(cargoConfirm_{encryptedBinary}, Bank_A)$

Step 6 - $Bank_A$:

$Accounts_{encrypted} = convertToString(Accounts_{encryptedBinary})$
$Account_B, Account_{OSP} + OTP = Accounts_{encrypted_{Key_{OSPAB}}}$
if OTP is correct **then**
send netPrice to $Account_B$
send commission to $Account_{OSP}$
end if

Table 2 Comparison between classical post-quantum cryptographic (PQC) approaches and the proposed quantum e-payment protocol

Feature	Classical cryptography + PQC	Our protocol
Active eavesdropping detection	NO	YES
Information-theoretic security	NO	YES
Message reordering detection	NO	YES
Quantum attack resilience	Limited	YES

detection of message reordering and correlation-based attacks, which are not inherently addressed by classical or PQC-based solutions. While PQC schemes offer partial resistance to quantum adversaries, the presented protocol provides stronger resilience by ensuring that any quantum attack results in detectable anomalies, thereby enhancing overall transaction security. In the presented protocol, information-theoretic security applies to the quantum channel and transmission integrity, while classical cryptographic components ensure the computational security of encrypted data.

5.1 Correctness

Each Bell state carries two classical bits between the two entities involved in the protocol. Suppose Alice wants to transmit a qubit to the OSP. Before data transmission, one of the entangled EPR pairs from Equation 1 in Sect. 3 must exist between Alice and the OSP.

Assume the EPR pair is $|\beta_{00}\rangle_{AOSP} = \frac{(|0_A 0_{OSP}\rangle + |1_A 1_{OSP}\rangle)}{\sqrt{2}}$

For n qubits, the equation is expressed by

$$|\beta_{00}\rangle_{A^n OSP^n}^{\oplus n} = \bigotimes_{i=1}^{n} |\beta_{00}\rangle_{A^i OSP^i}. \tag{3}$$

When Alice wants to send two classical bits $b_1 b_0 \in \{00, 01, 10, 11\}$, he must apply a Pauli operation (U) to his half-qubit. $|\Psi_{b_1 b_0}\rangle_{AOSP} = (U_{b_1 b_0} \oplus I_{OSP})|\beta_{00}\rangle_{AOSP}$

For n qubits, the equation is expressed by

$$U = \bigotimes_{i=1}^{n} U_{b_1^{(i)} b_0^{(i)}}. \tag{4}$$

The OSP performs a Bell state measurement on its own qubit and the qubit from Alice.

$$result \in \{00, 01, 10, 11\} Pr\left[result|\Psi_{b_1 b_0}\rangle\right] = |\langle Bell_{result}\rangle \Psi_{b_1 b_0}|^2 \tag{5}$$

Since $|\Psi_{b_1 b_0}\rangle = |Bell_{b_1 b_0}\rangle$, then

$$\langle Bell_{result}\rangle Bell_{b_1 b_0} = \delta_{k,(b_1 b_0)} Pr\left[result\right] = \delta_{k,(b_1 b_0)} \tag{6}$$

The measurement result of OSP is $b_1 b_0$

5.2 Threat model and security assumptions

We consider a powerful adversary Eve with quantum computational capabilities. Eve is assumed to have full access to the classical communication channel and partial access to the quantum channel. The adversary may perform passive eavesdropping

as well as active attacks, including intercept-and-resend, entangle-and-measure, and CNOT-based attacks.

The participating entities (Alice, Bob, banks, and the OSP) are assumed to be semi-honest, meaning that they follow the protocol correctly but may attempt to infer additional information from received data. The banking institutions and the OSP are assumed to be honest-but-curious and do not collude with external adversaries.

Denial-of-service attacks and physical attacks on quantum hardware are considered out of scope.

5.3 Security attacks

5.3.1 Intercept-and-resend attacks

Under the defined threat model, we show that any intercept-and-resend attack results in a detectable disturbance in Bell correlations, leading to a nonzero error rate at the receiver. In this attack, Eve intercepts the qubit sent by Alice, measures it, and generates another qubit, which she then sends to the OSP. The superdense coding states are mutually orthogonal. Therefore, if Eve measures a qubit in the $|0\rangle|1\rangle$ computational basis, she breaks the entanglement. This is because the reduced density matrix of the qubit sent by Alice is $\rho_A = \frac{I}{2}$. The information that can be obtained from a measurement depends on ρ_A. Eve's measurement result is unrelated to the classical message m; therefore, the classical information she can obtain is zero.

$$\chi = S(\sum_m p_m \rho_A^{(m)}) - \sum_m p_m S(\rho_A^{(m)}) = S(\frac{I}{2}) - S(\frac{I}{2}) = 0 \tag{7}$$

Eve reconstructs a qubit state based on her results and sends it to the OSP. The qubit sent by Eve and the corresponding qubit held by the OSP are not in the original Bell state. Therefore, the OSP's measurement $\rho_{OSP} = \frac{I}{2}$ yields a random result. This randomness enables Alice and the OSP to realise that the system is not secure.

5.3.2 CNOT attacks

We assume that Eve, an outside attacker, intercepts a qubit transmitted from Alice to the OSP in the presented protocol and uses this qubit as a control qubit to perform a CNOT attack. Eve attempts to obtain information about the transmitted data by observing the control qubit and creating her own target qubit. Eve prepares her own ancilla qubit in the state $|0\rangle_E$. Assume the transmitted qubit is $|\beta_{11}\rangle_{AOSP}$. Eve uses this qubit as the source and, with a CNOT attack, achieves the following.

$$\begin{aligned} |\beta_{11}\rangle_{AOSP}|0\rangle_E &= |\beta_{11}\rangle_{AOSP} \otimes |0\rangle_E \\ &= \frac{|0_A 1_{OSP}\rangle - |1_A 0_{OSP}\rangle}{\sqrt{2}}|0\rangle_E = \frac{|0_A 1_{OSP} 0_E\rangle - |1_A 0_{OSP} 0_E\rangle}{\sqrt{2}} \end{aligned} \tag{8}$$

After the CNOT attack, a three-partite entangled state arises.

$$\frac{|0_A 1_{OSP} 0_E\rangle - |1_A 0_{OSP} 0_E\rangle}{\sqrt{2}} \rightarrow CNOT \rightarrow \frac{|0_A 1_{OSP} 0_E\rangle - |1_A 0_{OSP} 1_E\rangle}{\sqrt{2}} \tag{9}$$

For Eve's density matrix $\rho_E = Tr_{AOSP}(\rho_{AOSPE})$, E has two orthogonal subcomponents, one $E = |0\rangle(AOSP = |01\rangle)$ and the other $E = |1\rangle(AOSP = |10\rangle)$. As the cross-terms ($|000\rangle\langle 111|$) vanish on BOSP due to orthogonality,

$$\rho_E = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{I}{2} \tag{10}$$

.

Because Eve's ancilla is mixed, any measurement she performs alone cannot yield classical information. Furthermore, Eve's CNOT attack disrupts Bell correlations. The AOSP subsystem changes from a pure Bell state to a statistical mixture; therefore, the OSP's measurements become corrupted, and the attack can be detected.

5.3.3 Entangle-and-measure attacks

Suppose the qubit transmitted from Alice to the OSP is initially $|\beta_{10}\rangle_{AOSP}$. Suppose an attacker, Eve, performs a unitary operation U_{AE} using Alice's qubit A and her own ancilla qubit $|0\rangle_E$ and then attempts to obtain information by measuring her own qubit.

$$\rho_{AOSP} = |\beta_{10}\rangle\langle\beta_{10}|_{AOSP}\rho_{AE}(|\beta_{10}\rangle_A \otimes |0\rangle_E) \tag{11}$$

When Eve is entangled with Alice's qubit, the density matrix is as follows.

$$\rho_{AOSPE} = (U_{AE} \otimes I_{OSP})(|\beta_{10}\rangle\langle\beta_{10}| \otimes |0\rangle\langle 0|_E)(U_{AE}^{\dagger} \otimes I_{OSP}) \tag{12}$$

In this case, the subsystem consisting of Alice and the OSP (AOSP) becomes entangled in the Bell basis due to Eve's interference. Consequently, the OSP's Bell measurements are corrupted, leading to an increase in the error rate.

Since Eve can only access subsystem E, her state is $rho_E = Tr_{AOSP}(rho_{AOSPE})$. When the trace is received over OSP,

$$\rho_E = Tr_A\left[U_{AE}(Tr_{OSP}(\rho_{AOSP}) \otimes |0\rangle\langle 0|_E)U_{AE}^{\dagger}\right] \tag{13}$$

Since $Tr_{OSP}(\rho_{AOSP}) = \rho_A = \frac{I_A}{2}$, then

$$\rho_E = Tr_A\left[U_{AE}(\frac{I_A}{2} \otimes |0\rangle\langle 0|_E)U_{AE}^{\dagger}\right] \tag{14}$$

Eve's U_{AE} operation results in ρ_E, which does not depend on the transmitted Bell state, as no parameters related to the initial Bell state remain in the value of ρ_E. Eve's entanglement weakens the Bell correlations between Alice and the OSP. Therefore,

the OSP's Bell measurement error rate increases. Message transmission is disrupted, and the attack is detected by both parties, but Eve does not obtain any information.

5.3.4 Inside one-way attacks

Suppose Bob intercepts and measures a qubit sent from Alice to the OSP. If Bob has only one-way access to the sent qubit, the resulting state will be maximally mixed, $\rho = \frac{I}{2}$. Since the Holevo information equals zero, Bob cannot obtain any classical information. However, if Bob participated in the initial preparation of the shared state and has access to the purification, or if he possesses both Alice's and the OSP's qubits, he can obtain the data. To prevent this, the presented protocol encrypts all communication between the parties using shared secret keys after the initial secure key distribution. This ensures that even if data are obtained through an insider attack, no meaningful message can be extracted. Furthermore, message complexity increases if the encrypted data bits are transmitted in a random order rather than sequentially.

5.4 Security features

5.4.1 Anonymity

The buyer and seller IDs, ID_A and ID_B, are randomly assigned by the OSP during the Initialisation Phase. Each party's ID is stored as identity data and is known only to the party itself and the OSP. In the presented protocol, ID_A and ID_B appear only in the m1 data within the $order_{message}$ sent by Alice to the OSP during the purchase order creation phase. However, the m1 data are not transmitted explicitly. It is first encrypted with the shared secret key Key_{AOSP}, shared between Alice and the OSP, then converted to binary format, and transmitted over a quantum line using superdense coding, a secure quantum communication protocol. Because any measurement made on the quantum line before it reaches the receiver would interfere with the receiver's measurement, and because the m1 data use ID data representing the parties rather than personal data, identity leakage is prevented, and the anonymity of the parties is ensured.

5.4.2 Unforgeability

For an external attacker to impersonate one party in the protocol and send a message to another, they would need access to the secret keys exchanged between the parties. However, these keys are transmitted using superdense coding. Instead of obtaining one of the keys, the attacker might intercept the quantum sequence sent by one party and transmit a randomly generated, fake quantum sequence to the other party. This would be detected by examining the control bits in the quantum sequence. When the quantum sequence is converted to an encrypted format, the data cannot be decrypted with the shared key between the two parties, thereby revealing noise or an attack.

5.4.3 Undeniability

The presented protocol designates banks as central entities for payment processing between parties. When Alice places an order, she must send a confirmation message to $Bank_A$ for the order price. A successful order is not created until $Bank_A$ receives this confirmation. If she denies receiving the order, the OSP can verify delivery by checking the shipping information. After delivery, $Bank_A$ sends the order commission to $Bank_{OSP}$ and the net order price to $Bank_B$. If Bob says the money has not arrived in his account, this can be easily verified by checking his bank transactions. The protocol achieves operational non-repudiation by ensuring that all transactions are recorded and verified by the OSP, making denial of participation impractical within the system's operational framework. Cryptographic non-repudiation based on digital signatures is not provided. Instead, the protocol ensures operational non-repudiation through centralised banking records and transaction verification.

6 Performance

Two-particle entangled states, which are easier to prepare, are used as quantum sources. As shown in Table 3, in the presented protocol, two-particle entangled states serve as quantum sources in the orderly binary send and random binary send methods for message transmission. The presented protocol also uses Pauli and H gates as operators, and two-particle, single-particle, and Bell states for measurement operations.

Since banks are central entities in our protocol, payment transactions are recorded by them, and data are not separately recorded on the blockchain to prevent duplication.

In the presented protocol, all message transmissions between the sender and receiver are carried out using either the orderly or random binary send method. Assume that the two-bit data '11' is transmitted from the sender to the receiver via q_0 and q_1 using the orderly binary send method. The operations shown in Figure 3 are performed sequentially.

Suppose q_2 and q_3 be two qubits in the state $|00\rangle$. First, the Hadamard gate is applied to q_2.

$$
\begin{aligned}
H|0\rangle &= \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix}\right) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\\
H|0\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}}\\
H|00\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}}|0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}
\end{aligned}
\tag{15}
$$

Then, q_2 and q_3 pass through the CNOT gate.

$$
\frac{|00\rangle + |10\rangle}{\sqrt{2}} \rightarrow CNOT \rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{16}
$$

Table 3 Comparisons of our proposed protocol with previous quantum e-payment protocols

Protocols	Quantum resources	Operators	Measurements	Trusted third-party	Blockchain
Guo et al. [21]	3-PES, S-PS	P, H	B-SM, S-PM	NO	YES
Tiliwalidi et al. [29]	6-PES	P	3-PM, S-PM, B-SM	NO	NO
Zhang et al. [33]	6-PES	P	B-SM, S-SM, G-SM	NO	YES
Zhang et al. [31]	4-PES	P	B-SM, S-PM	YES	NO
Nie et al. [32]	4-PES	P	S-PM, 3-PM	NO	NO
Guo et al. [43]	S-PS	P	S-PM	YES	NO
Xie et al. [35]	4-PES	P	B-SM, S-PM	NO	NO
Our protocol	2-PES	P, H	2-PM, S-PM, B-SM	YES	NO

Note: S-PS, 2-PES, 3-PES, 4-PES, and 6-PES denote single-particle states, 2-particle entangled states, 3-particle entangled states, 4-particle entangled states, and 6-particle entangled states, respectively. Furthermore, P and H represent Pauli and H-gate operators, respectively. In addition, S-PM, 2-PM, 3-PM, B-SM, and G-SM denote single-particle measurements, 2-particle measurements, 3-particle measurements, Bell state measurements, and GHZ-state measurements, respectively

For the $|\beta_{00}\rangle$ bell state, q_2 and q_3 pass through the gates $Z^{(q_0 \oplus q_2)}$ and $X^{(q_1 \oplus q_3)}$, respectively. If the two bits to be sent are '11,' both the Z and X gates are applied to q_2. If '01' is to be sent, only the Pauli X gate is applied to q_2, corresponding to Z^1 and X^0. If '10' is to be sent, only the Pauli Z gate is applied to q_2, corresponding to Z^0 and X^1. If '00' is to be sent, neither gate is applied to q_2.

To send '11,' q_2 is first passed through the Pauli Z gate.

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \rightarrow Z \rightarrow \frac{|00\rangle - ||11\rangle}{\sqrt{2}} \tag{17}$$

Then, q_2 is passed through the Pauli X gate.

$$\frac{|00\rangle - |11\rangle}{\sqrt{2}} \rightarrow X \rightarrow \frac{|10\rangle - |01\rangle}{\sqrt{2}} \tag{18}$$

At the receiver side, q_2 and q_3 pass through the CNOT gate.

$$\frac{|10\rangle - |01\rangle}{\sqrt{2}} \rightarrow CNOT \rightarrow \frac{|11\rangle - |01\rangle}{\sqrt{2}} \tag{19}$$

Then, the Hadamard gate is applied to q_2.

$$\frac{|11\rangle - |01\rangle}{\sqrt{2}} \rightarrow H \rightarrow \frac{\frac{(|0\rangle - |1\rangle)|1\rangle}{\sqrt{2}} - \frac{(|0\rangle + |1\rangle)|1\rangle}{\sqrt{2}}}{\sqrt{2}} = \frac{|01\rangle - |11\rangle - |01\rangle - |11\rangle}{2} = \frac{2|11\rangle}{2} = -|11\rangle \tag{20}$$

The '-' sign represents the global phase difference and does not affect the measurement results. The '11' sent by the sender corresponds to the '11' measured by the receiver.

Assume that the random binary send method is used to transmit messages between the sender and receiver. The steps in Figure 3 are performed in order.

On the sender side, the sender first prepares an EPR pair using qubits q_2 and q_3, creating a Bell state. The sender then prepares two particles, q_0 and q_1, applies Hadamard gates to these qubits, and performs a measurement. The random binary states q_0 and q_1 obtained from the measurement are compared with the bits of the message to be transmitted. If two consecutive bits in the message match the randomly generated q_0 and q_1 states, this binary data is transmitted to the receiver. If not, the gate application, measurement, and comparison processes are repeated on qubits q_0 and q_1. This process continues cyclically until the entire binary message is sent.

Assume that a Bell state is created using q_2 and q_3 is $|\beta_{00}\rangle$, and the measurement result of q_0 and q_1 is '00,' which is included in the binary message to be transmitted.

On the sender side, q_0 and q_2 are passed through an XOR gate.

$q_0 \oplus q_2 \rightarrow 0 \oplus 0 \oplus 0$

As the result is 0, gate Z is not applied to q_2.

Then q_1 and q_3 are passed through the XOR gate.

$q_1 \oplus q_3 \rightarrow 0 \oplus 0 \oplus 0$

As the result is 0, gate X is not applied to q_2.

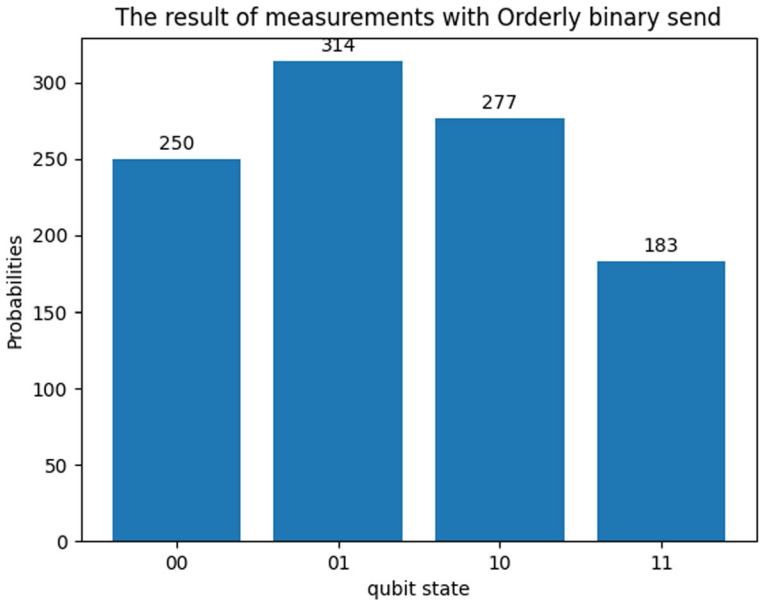

Fig. 4 The result of the circuit being executed with orderly binary send method

At the receiver side, q_2 and q_3 are passed through the CNOT gate.

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \rightarrow CNOT \rightarrow \frac{|00\rangle + |10\rangle}{\sqrt{2}} \tag{21}$$

Then, the Hadamard gate is applied to q_2.

$$\begin{aligned} &\frac{|00\rangle + |10\rangle}{\sqrt{2}} \rightarrow H \rightarrow \frac{\frac{(|0\rangle+|1\rangle)|0\rangle}{\sqrt{2}} + \frac{(|0\rangle-|1\rangle)|0\rangle}{\sqrt{2}}}{\sqrt{2}} \\ &= \frac{|00\rangle + |10\rangle + |00\rangle - |10\rangle}{2} = \frac{2|00\rangle}{2} = |00\rangle \end{aligned} \tag{22}$$

The sender transmits a value of '00,' which corresponds to the receiver obtaining a value of '00.'

Figure 4 shows that the orderly binary send method is executed for a total of 1024 iterations during the sequential transmission of a 256-byte message from the sender to the receiver without adding any false bits.

Figure 5 shows the total number of times the random binary send method was executed when the same message was randomly transmitted. The random binary send method generated the binary numbers 00, 01, 10, and 11 a total of 352, 314, 341, and 339 times, respectively. Therefore, the method was executed 1346 times in total to transmit the same message between the two parties.

The second, third, and fourth columns of Table 4 show the increased binary data length resulting from adding a pseudo-bit after every 2, 4, and 8 bits, respectively.

Table 4 Comparison of binary data length resulting from pseudo-bit operations using orderly or random methods

Method	No pseudo-bits	After every 2 bits	After every 4 bits	After every 8 bits
Binary length	8n	12n	10n	9n
Orderly binary send	4n	6n	5n	$\frac{9n}{2}$
Random binary send	5n-7n	9n-10n	7n-8n	6n-7n

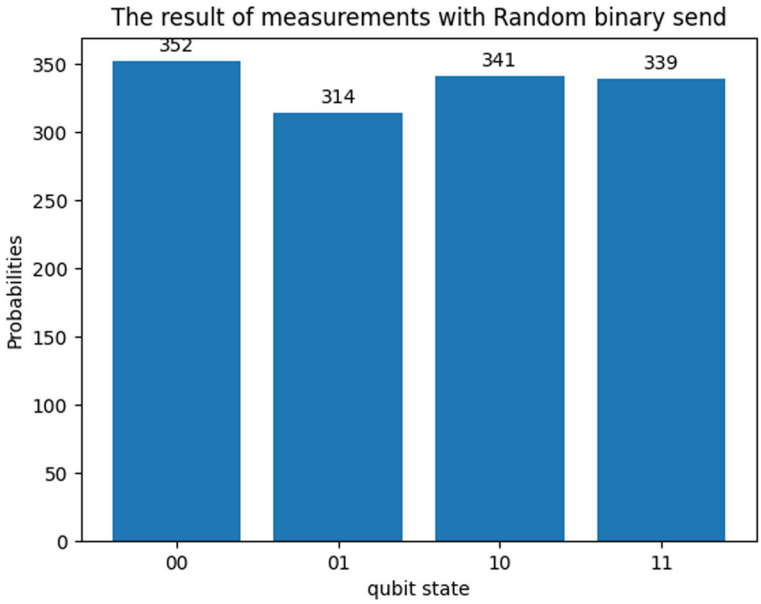

Fig. 5 The result of the circuit being executed with random binary send method

As shown in the first row of Table 4, if the encrypted message is n characters long, it will occupy 8n bits in binary. Adding a pseudo-bit every 2 bits increases the message length to 12n; every 4 bits, to 10n; and every 8 bits, to 9n. As indicated in the second row of the table, the orderly binary send method, which transmits 2 bits of classical data sequentially in each superdense coding operation, must be executed half as many times as the number of bits to be transmitted. However, as shown in the third row, the random binary send method must be executed more times than the orderly binary send method to transmit the same amount of data. This is because, in the random binary send method, two randomly generated bits must first be checked on the sender's side to ensure they match two consecutive bits in the message before transmission to the receiver. For every two bits that do not match, the method must be re-executed.

6.1 Limitations and practical considerations

The performance evaluation assumes ideal quantum channels without considering decoherence, quantum memory limitations, or channel noise. While current quantum hardware may not support large-scale deployment of the presented protocol, the design is intended for future quantum-enabled financial infrastructures. Addressing noise tolerance and error correction remains an important direction for future research.

7 Conclusion

Unlike decentralised quantum payment schemes, a centralised architecture enables regulatory compliance, dispute resolution, transaction auditing, and commission management, which are mandatory requirements in real-world financial systems.

In this study, we propose a novel centralised e-payment protocol based on superdense coding and secret key encryption. The presented protocol initially defined shared secret keys for all transmission processes between the parties. This ensures message security by encrypting transmissions.

Compared with other related protocols, our protocol offers two distinct data transmission methods—orderly and random—to enhance message transmission security. For messages of equal length, the number of times each method is run shows that random data transmission is 50% more than orderly data transmission, whether no pseudo-bits are added or a pseudo-bit is added every 4 bits. Random data transmission is approximately 60% more when a pseudo-bit is added every two bits, and about 40% more when a pseudo-bit is added every eight bits.

Our protocol only uses two-particle entangled states and Bell state measurements, which can reduce the complexity of quantum resources. Through theoretical security features, the presented protocol is analysed in terms of anonymity, unforgeability, and undeniability. It is also demonstrated that it is resilient against intercept-and-resend, CNOT, entangle-and-measure, and inside one-way attacks, and that it meets the intended security requirements.

Author contributions Zeynep Çelik and Hüseyin Bodur conducted the study together and co-authored the article.

Funding Open access funding provided by the Scientific and Technological Research Council of Türkiye (TÜBİTAK).

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have influenced the work reported in this study.

References

1. Lawal, O., Vincent, O., Agboola, A., Folorunso, O.: An improved hybrid scheme for e-payment security using elliptic curve cryptography. Int. J. Inf. Technol. **13**(1), 139–153 (2021)

2. Yang, J.-H., Chang, Y.-F., Chen, Y.-H.: An efficient authenticated encryption scheme based on ECC and its application for electronic payment. Inf. Technol. Control **42**(4), 315–324 (2013)
3. Chaudhry, S.A., Farash, M.S., Naqvi, H., Sher, M.: A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography. Electron. Commer. Res. **16**(1), 113–139 (2016)
4. Okediran, T., Vincent, O., Abayomi-Alli, A., Adeniran, O.: Securing the perceptual layer of e-payment-based internet of things devices using elliptic curve cryptography over binary field. J. Supercomput. **80**(15), 21592–21614 (2024)
5. Luong, T.-D., Vu, T.-V.: An efficient privacy-preserving recommender system based on elliptic curve. Ann. Op. Res. 1–29 (2025)
6. Gorantla, V.A.K., Gude, V., Sriramulugari, S.K., Yuvaraj, N., Yadav, P.: Utilizing hybrid cloud strategies to enhance data storage and security in e-commerce applications. In: 2024 2nd International Conference on Disruptive Technologies (ICDT), pp. 494–499. IEEE (2024)
7. Tariq, U., Jaafar, F., Malik, Y.: Detecting and mitigating adversarial perturbations to improve e-commerce security. In: 2024 IEEE/ACM International Conference on Big Data Computing, Applications and Technologies (BDCAT), pp. 334–341. IEEE (2024)
8. Ahuja, B., Prabha, C., Garg, G.: Emerging technologies in e-commerce security. Strateg. Innov. AI ML E-Comm. Data Sec. 235–260 (2025)
9. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev. **41**(2), 303–332 (1999)
10. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing, pp. 212–219 (1996)
11. Tiwo, O.J., Adesokan-Imran, T.O., Babarinde, D.C., Oyekunle, S.M., Olutimehin, A.T., Olaniyi, O.O.: Advancing security in cloud-based patient information systems with quantum-resistant encryption for healthcare data. Asian J. Res. Comput. Sci. **18**(4), 187–208 (2025)
12. Kar, A.K., He, W., Payton, F.C., Grover, V., Al-Busaidi, A.S., Dwivedi, Y.K.: How could quantum computing shape information systems research–An editorial perspective and future research directions. Elsevier (2025)
13. Naik, A.S., Yeniaras, E., Hellstern, G., Prasad, G., Vishwakarma, S.K.L.P.: From portfolio optimization to quantum blockchain and security: a systematic review of quantum computing in finance. Financ. Innov. **11**(1), 1–67 (2025)
14. Long, G.-L., Liu, X.-S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A **65**(3), 032302 (2002)
15. Deng, F.-G., Long, G.L., Liu, X.-S.: Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block. Phys. Rev. A **68**(4), 042317 (2003)
16. Zhang, W., Ding, D.-S., Sheng, Y.-B., Zhou, L., Shi, B.-S., Guo, G.-C.: Quantum secure direct communication with quantum memory. Phys. Rev. Lett. **118**(22), 220501 (2017)
17. Pan, D., Long, G.-L., Yin, L., Sheng, Y.-B., Ruan, D., Ng, S.X., Lu, J., Hanzo, L.: The evolution of quantum secure direct communication: on the road to the Ginternet. IEEE Commun. Surv. Tutor. **26**(3), 1898–1949 (2024)
18. Qi, Z., Li, Y., Huang, Y., Feng, J., Zheng, Y., Chen, X.: A 15-user quantum secure direct communication network. Light: Sci. Appl. **10**(1), 183 (2021)
19. Yang, Y., Li, Y., Li, H., Wu, C., Zheng, Y., Chen, X.: A 300-km fully-connected quantum secure direct communication network. Sci. Bull. **70**(9), 1445–1451 (2025)
20. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. Theoret. Comput. Sci. **560**, 7–11 (2014)
21. Gou, X.-L., Shi, R.-H., Gao, W., Wu, M.: A novel quantum e-payment protocol based on blockchain. Quantum Inf. Process. **20**(5), 192 (2021)
22. Xiaojun, W.: An e-payment system based on quantum group signature. Phys. Scr. **82**(6), 065403 (2010)
23. Xiaojun, W., Zhe, N.: An e-payment system based on quantum blind and group signature. In: 2010 Second International Symposium on Data, Privacy, and E-Commerce, pp. 50–55. IEEE (2010)
24. Wen, X., Chen, Y., Fang, J.: An inter-bank e-payment protocol based on quantum proxy blind signature. Quantum Inf. Process. **12**(1), 549–558 (2013)
25. Fatonah, S., Yulandari, A., Wibowo, F.W.: A review of e-payment system in e-commerce. J. Phys: Conf. Ser. **1140**, 012033 (2018). (**IOP Publishing**)
26. Li, E., Shi, R.-H., Li, K., Li, Y.: Measurement-device-independent quantum protocol for e-payment based on blockchain. Quantum Inf. Process. **22**(1), 40 (2023)

27. Li, G.-D., Luo, J.-J., Wang, Q.-L.: Twin-field quantum encryption protocol for e-payment based on blockchain. Quantum Inf. Process. **22**(12), 430 (2023)
28. Wang, Q., Liu, J., Li, G., Han, Y., Zhou, Y., Cheng, L.: A measurement-device-independent quantum secure digital payment. Phys. A **655**, 130178 (2024)
29. Tiliwalidi, K., Zhang, J.-Z., Xie, S.-C.: A multi-bank e-payment protocol based on quantum proxy blind signature. Int. J. Theor. Phys. **58**(10), 3510–3520 (2019)
30. Song, Y., Wu, Y., Wu, S., Li, D., Wen, Q., Qin, S., Gao, F.: A quantum federated learning framework for classical clients. Sci. China Phys. Mech. Astron. **67**(5), 250311 (2024)
31. Zhang, J.-Z., Yang, Y.-Y., Xie, S.-C.: A third-party e-payment protocol based on quantum group blind signature. Int. J. Theor. Phys. **56**(9), 2981–2989 (2017)
32. Niu, X.-F., Zhang, J.-Z., Xie, S.-C., Chen, B.-Q.: A third-party e-payment protocol based on quantum multi-proxy blind signature. Int. J. Theor. Phys. **57**(8), 2563–2573 (2018)
33. Zhang, J.-L., Hu, M.-S., Jia, Z.-J., Wang, L.-P.: A novel e-payment protocol implented by blockchain and quantum signature. Int. J. Theor. Phys. **58**(4), 1315–1325 (2019)
34. Gupta, A., Chandra, G.V., Das, N., Paul, G.: An efficient and secure quantum blind signature-based electronic cash transaction scheme. IET Quantum Commun. **5**(4), 619–631 (2024)
35. Xie, S.-C., Niu, X.-F., Zhang, J.-Z.: An improved quantum e-payment system. Int. J. Theor. Phys. **59**(2), 445–453 (2020)
36. Yu, H., Zhang, Q., Li, L.: Certificateless anti-quantum blind signcryption for e-cash. J. Ind. Inf. Integr. **40**, 100632 (2024)
37. Qin, L., Liu, B., Gao, F., Huang, W., Xu, B., Li, Y.: Decoy-state quantum private query protocol with two-way communication. Phys. A **633**, 129427 (2024)
38. Schiansky, P., Kalb, J., Sztatecsny, E., Roehsner, M.-C., Guggemos, T., Trenti, A., Bozzio, M., Walther, P.: Demonstration of quantum-digital payments. Nat. Commun. **14**(1), 3849 (2023)
39. Yaga, D., Mell, P., Roby, N., Scarfone, K.: Blockchain technology overview. arXiv:1906.11078 (2019)
40. Guo, L., Xie, H., Li, Y.: Data encryption based blockchain and privacy preserving mechanisms towards big data. J. Vis. Commun. Image Represent. **70**, 102741 (2020)
41. Bennett, C.H., Wiesner, S.J.: Communication via one-and two-particle operators on Einstein–Podolsky–Rrosen states. Phys. Rev. Lett. **69**(20), 2881 (1992)
42. Westfall, L., Leider, A.: Superdense coding step by step. In: Future of Information and Communication Conference, pp. 357–372. Springer, Cham (2019)
43. Guo, X., Zhang, J.-Z., Xie, S.-C.: A trusted third-party e-payment protocol based on quantum blind signature without entanglement. Int. J. Theor. Phys. **57**(9), 2657–2664 (2018)