Uluslararası Fen Araştırmalarında Yenilikçi Yaklaşımlar Dergisi
International Journal of Innovative Approaches in Science Research 2024, Vol. 8 (2), 90-112
https://doi.org/10.29329/ijiasr.2024.1054.5

Original article

Quantum Digital Signature Generation with Quantum Continuous Variables

Cumali Yaşar [a,*] & Can Aktaş [b]

[a] Department of Computer Education and Instructional Technology, Faculty of Education, Çanakkale Onsekiz Mart University, Çanakkale, Türkiye
[b] Department of Mathematics, Faculty of Science, Çanakkale Onsekiz Mart University, Çanakkale, Türkiye

Abstract

Ensuring the security of digital communication and data transfer has become essential in the modern era. Classical cryptographic techniques are increasingly vulnerable due to advances in quantum technologies and algorithms. Consequently, quantum computers and quantum communication offer promising solutions for secure data transfer and encryption. This study explores the generation of Quantum Digital Signatures (QDS) using Quantum Continuous Variables (QCV), providing a novel approach to secure digital signature technologies.

The paper outlines the core principles of QDS generation with QCV, detailing the signature creation and verification processes. It highlights the advantages of this technology in secure communication and data transfer and discusses potential security vulnerabilities and future development prospects. Quantum Continuous Variables (QCVs), typically used in quantum optical systems, represent physical quantities with continuous spectra, such as the wavelength or phase of light. These variables enable efficient and secure quantum information processing and communication.

Despite significant progress in quantum cryptography protocols using QCVs, practical application and optimization of these technologies face numerous challenges. These include complexities in preparing and measuring quantum states, managing quantum errors, and achieving higher efficiency and security standards. Moreover, the practical applications of QCV in industrial contexts remain limited, highlighting the need for further experimental and applied research.

The methodology for generating QDS using QCVs involves employing specific quantum states, such as coherent and squeezed states. The process includes key distribution, signature creation and verification, and addressing potential quantum attacks. The system model comprises a sender (Alice), a receiver (Bob), and an arbiter (Charlie), facilitating secure and authenticated message transmission.

Keywords: Quantum Digital Signature, Continuous Variables, Quantum Cryptography, Coherent States, Squeezed States, Quantum Communication, Secure Data Transfer, Quantum Computing, Phase Shift, Quantum Key Distribution (QKD).

Received: 31 August 2023 * **Accepted:** 30 March 2024 * **DOI:** https://doi.org/10.29329/ijiasr.2024.1054.5

[*] **Corresponding author:**

Yaşar Cumali is an Lecturer in the Department of Computer Education and Instructional Technology at Çanakkale Onsekiz Mart University in Çanakkale, Türkiye. His research interests include Artificial Intelligence, Educational Technologies, and Software Development. He has lived, worked, and studied in Çanakkale, Türkiye.
Email: cyasar@comu.edu.tr

INTRODUCTION

In today's world, the security of digital communication and data transfer has become a fundamental necessity (Adesso vd., 2007; Braunstein & van Loock, 2005). Classical cryptographic techniques are increasingly vulnerable due to advancements in quantum technologies and algorithms. As a result, quantum computers and quantum communication emerge as promising solutions for secure data transfer and encryption. In this context, the generation of Quantum Digital Signatures (QDS) using Quantum Continuous Variables (QCV) adds a new dimension to secure digital signature technologies (Booth, 2021).

This paper will detail the core principles of QDS generation with QCV, explaining the signature creation and verification processes. We will highlight the advantages of this technology in secure communication and data transfer and discuss potential security vulnerabilities and future development prospects. Ultimately, we emphasize that QDS, leveraging QCV, has the potential to shape future security standards in quantum information and quantum computing (Braunstein & van Loock, 2004; Deng vd., 2016; Diep vd., 2020).

Quantum computing, utilizing the unique properties of quantum mechanics, revolutionizes information processing and storage methods. Quantum computers surpass classical computers by exploiting phenomena such as superposition and entanglement (Adesso vd., 2007; Ben-David & Sattath, 2016). Quantum signatures play a particularly important role in this new paradigm. Quantum digital signatures(Gottesman & Chuang, 2001a) use the principles of quantum mechanics to authenticate and ensure the integrity of digital messages or documents, providing a robust tool to verify the sender's identity and ensure that the transmitted message has not been altered (Buck vd., 2021a).

In this study, the generation of QDS using QCV is crucial for the future of secure digital signature technologies. Continuous variables, used in quantum optical systems, typically represent physical quantities with continuous spectra, such as the wavelength or phase of light (Deng vd., 2016). These variables can represent quantum states used in quantum information processing and communication. One of the advantages of working with continuous variables is that quantum information processing and communication are generally more efficient and secure (Braunstein & van Loock, 2004).

This study aims to present the fundamental principles and application methods of generating QDS using QCV. By leveraging the quantum mechanical properties and principles of continuous variables, this approach provides an effective way to create and verify digital signatures. This framework can be particularly valuable in practical applications where information security is paramount, such as in quantum information processing and quantum communication (Braunstein & van Loock, 2005).

This Figure-1 is a mindmap diagram that outlines the key aspects of Quantum Digital Signatures (QDS) using Quantum Continuous Variables (QCV). It highlights the importance of digital communication security, the vulnerabilities of classical cryptographic techniques, and the advancements in quantum technologies and algorithms. The diagram also covers the principles of QDS generation, the processes for signature creation and verification, and the advantages and potential security vulnerabilities of QDS with QCV. Lastly, it discusses future development prospects and concludes with the potential of QDS to set future security standards in quantum information and computing (Buck vd., 2021b).

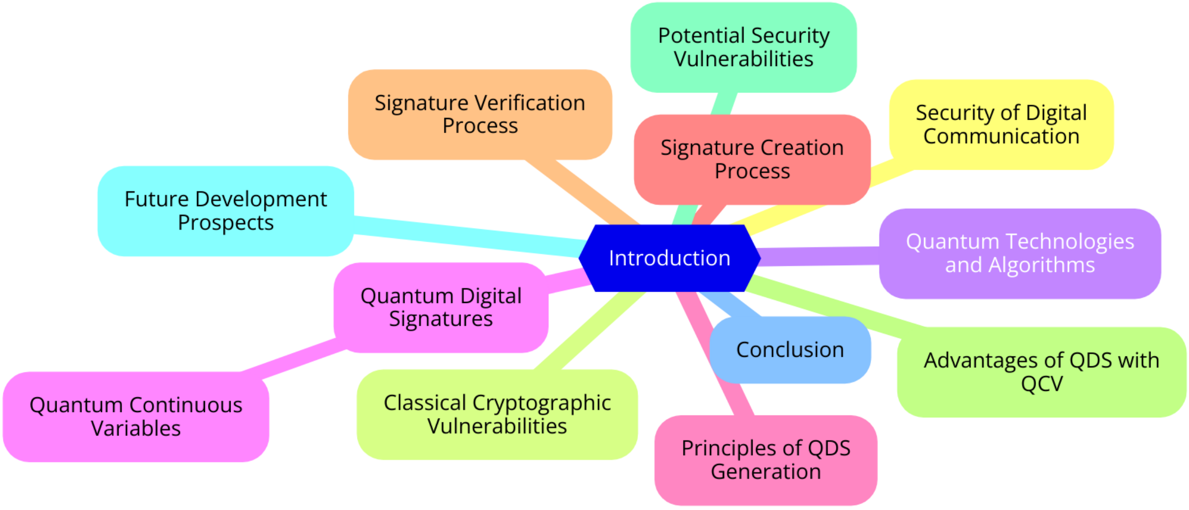

Potential Security Vulnerabilities
Signature Verification Process
Security of Digital Communication
Signature Creation Process
Future Development Prospects
Introduction
Quantum Technologies and Algorithms
Quantum Digital Signatures
Conclusion
Advantages of QDS with QCV
Quantum Continuous Variables
Classical Cryptographic Vulnerabilities
Principles of QDS Generation

Figure 1. Introduction to Quantum Digital Signatures (QDS) Using Quantum Continuous Variables (QCV)(OpenAI, 2020)

In conclusion, this study highlights the potential of QDS using QCV to set future security standards in quantum information and computing. While there are technological challenges and costs associated with these technologies, ongoing research and development are essential to address these limitations and fully exploit the potential of QDS in various practical applications.

Definitions of Concepts

Quantum Continuous Variables (QCV): Quantum Continuous Variables are quantum systems characterized by continuous spectra of their physical properties, such as the amplitude and phase of a light beam or the position and momentum of an electron. QCVs are often used in quantum optical systems, where the number of photons is uncertain (Diep vd., 2020).

Quantum Continuous Variables are characterized by continuous spectra of their physical properties. They are often represented using quadrature operators (Booth, 2021; Pfister, 2019):

$$\hat{x} = \frac{\hat{a} + \hat{a}^\dagger}{\sqrt{2}}, \qquad \hat{p} = \frac{\hat{a} - \hat{a}^\dagger}{i\sqrt{2}} \tag{1}$$

where $\hat{a}$ and $\hat{a}^\dagger$ are the annihilation and creation operators.

Quantum Discrete Variables (QDV): Quantum Discrete Variables refer to quantum systems with discrete values, such as the spin or photon number. QDVs are commonly modeled using qubits (quantum bits), which are two-level systems representing two possible states (Jain vd., 2022).

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2}$$

where $|\alpha|^2 + |\beta|^2 = 1$.

Quantum Digital Signature (QDS): A Quantum Digital Signature is a method of ensuring the authenticity and integrity of digital messages or documents using quantum mechanics principles. QDS leverages quantum properties to provide a secure way to verify the sender's identity and ensure the message has not been altered (Gottesman & Chuang, 2001b).

Coherent States: Coherent states are special quantum states of the quantum harmonic oscillator that behave similarly to classical harmonic oscillators. They are essential in quantum optics for describing the quantum nature of light and serve as a bridge between classical and quantum behaviors (Braunstein & van Loock, 2004; Buck vd., 2021b).

A coherent state $|\alpha\rangle$ is an eigenstate of the annihilation operator $\hat{a}$:

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle \tag{3}$$

Coherent states can be expressed as:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{4}$$

where α is a complex number.

Squeezed States: Squeezed states are quantum states where the uncertainty in one property (like position or momentum) is reduced at the expense of increased uncertainty in the conjugate property. These states are used in precision measurements and quantum information processing (Yan-Yan vd., 2018).

Squeezed states are generated by applying the squeeze operator $\hat{S}(r)$ to the vacuum state:

$$|z\rangle = \hat{S}(r)|0\rangle \tag{5}$$

where the squeeze operator is:

$$\hat{S}(r) = e^{\frac{r}{2}(\hat{a}^2 - \hat{a}^{\dagger 2})} \tag{6}$$

and r is the squeezing parameter.

Quantum Key Distribution (QKD): Quantum Key Distribution is a secure communication method using quantum mechanics principles to enable two parties to produce a shared random secret key, which can then be used to encrypt and decrypt messages. QKD is known for its ability to detect any eavesdropping on the communication channel.

QKD protocols, such as BB84, use quantum states to establish a secure key. The BB84 protocol involves encoding bits in the polarization states of photons:

$$|0\rangle, |1\rangle, |+\rangle, |-\rangle$$

where $|+\rangle = \frac{1}{\sqrt{2}}\,(\,|0\rangle + |1\rangle\,)$ and $|-\rangle = \frac{1}{\sqrt{2}}(\,|0\rangle - |1\rangle)$

Homodyne and Heterodyne Measurements: Homodyne and heterodyne measurements are techniques used in quantum optics to measure the properties of quantum states, such as the phase and amplitude of light. These measurements are crucial for quantum state verification and quantum information protocols.

Homodyne detection measures the quadrature $\hat{x}$ or $\hat{p}$:

$$\hat{x}_\theta = \hat{x}cos\theta + \hat{p}\mathrm{sin}\theta \tag{7}$$

Gaussian Modulation: Gaussian modulation involves modulating both the amplitude and phase of a quantum state to carry complex information. This modulation technique is commonly used in QCV systems for efficient and secure information transfer (Adesso vd., 2007).

Gaussian modulation of a quantum state involves displacing the state in phase space using the displacement operator $\widehat{D}(\alpha)$:

$$\widehat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - a^*\hat{a}} \tag{8}$$

where α is a complex number representing the displacement(Grosshans vd., 2003).

Phase Modulation (PM): Phase Modulation is a method of encoding information in the phase of a quantum state. It is used to create specific quantum states that carry information based on their phase properties (Clarke vd., 2012).

Phase modulation is achieved by applying a phase shift operator $\hat{P}(\phi)$ to the quantum state (Clarke vd., 2012):

$$\hat{P}(\phi) = e^{i\phi\hat{a}^\dagger\hat{a}}$$

where ϕ is the phase shift.

Amplitude Modulation (AM): Amplitude Modulation is a technique where the amplitude of a quantum state is adjusted to encode information. This method allows the quantum state to carry data through its intensity.

These definitions provide a foundational understanding of the key concepts involved in the study and application of Quantum Digital Signatures using Quantum Continuous Variables.

Wigner Function (Wootters, 1987): The Wigner function is a quasi-probability distribution used in quantum mechanics to represent a quantum state in phase space. It serves as a bridge between quantum and classical descriptions of a system.

For a quantum state described by the density matrix ρ , the Wigner function $W(x, p)$ is defined as:

$$W(x,p) = \frac{1}{\pi\hbar}\int_{-\infty}^{\infty} \langle x + y|\rho|x - y\rangle e^{-2ipy/\hbar} dy$$

where:

x is the position.

p is the momentum.

$\hbar$ is the reduced Planck constant.

$|\ x\ \rangle$ is the position eigenstate.

$\langle x + y|\rho|x - y\rangle$ is the matrix element of the density operator in the position representation.

For Pure States: For a pure quantum state $|\psi\rangle$ with wave function $\psi(x)$, the Wigner function is:

$$W(x,p) = \frac{1}{\pi\hbar}\int_{-\infty}^{\infty} \psi^*(x + y)\psi(x - y)e^{-2ipy/\hbar} dy$$

where $\psi(x)$ is the wave function and $\psi^*(x)$ is its complex conjugate.

For Coherent States: For a coherent state $|\alpha\rangle$ with complex parameter α, the Wigner function is:

$$W(\alpha) = \frac{2}{\pi}\exp(-2|\alpha - \alpha_0|^2)$$

where α_0 is the center of the coherent state in phase space.

In summary, the Wigner function is a vital tool in the generation and verification of digital signatures using quantum continuous variables, providing essential insights into the quantum states involved (Wootters, 1987).

MATERIALS and METHODS

System Model

The methodology for generating and utilizing quantum digital signatures (QDS) using continuous variables (CV) is presented in this study. The method involves the use of specific states of quantum mechanical systems, such as coherent states and squeezed states (Buck vd., 2021a; Deng vd., 2016).

Our system model consists of three participants: a message sender (Alice), a message receiver (Bob), and an arbiter (Charlie). This model represents a scenario where Alice wants to securely transmit a message to Bob, and Charlie verifies the authenticity and security of this communication.

This diagram Figure-2 represents a scenario where Alice wants to securely transmit a message to Bob, and Charlie verifies the authenticity and security of this communication.

- **Alice**: The message sender.
- **Bob**: The message receiver.
- **Charlie**: The arbiter who verifies the authenticity and security of the message.

The communication flow is as follows:

1. Alice requests Charlie to verify her message.
2. Charlie confirms the message verification to Alice.
3. Alice sends the message to Bob.
4. Bob asks Charlie to confirm the message's authenticity.
5. Charlie confirms the authenticity of the message to Bob.

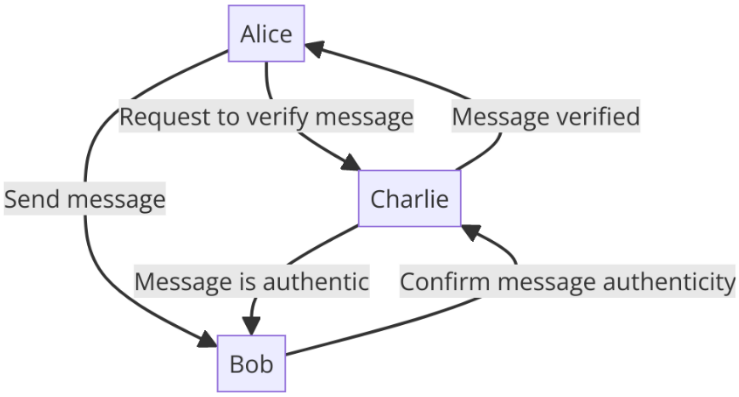


Figure 2. Secure Message Transmission Between Alice, Bob, and Charlie (OpenAI, 2020)

Quantum State Selection and Manipulation(Clarke vd., 2012)

State Selection: Alice selects a specific quantum state to sign a message. In this study, both coherent states and squeezed states are utilized. These states are typically used in the analysis of continuous variable quantum systems.

Example (Johansson vd., 2012a): Let's consider an example where Alice chooses a coherent state with $\alpha = 1 + i$.

State Selection (Coherent State):

$$\alpha = 1 + i.$$

The coherent state $\mid \mathbf{1} + \boldsymbol{i}\rangle$ is:

$$|1 + i\rangle = e^{-\frac{|1+i|^2}{2}} \sum_{n=0}^{\infty} \frac{(1 + i)^n}{\sqrt{n!}} |n\rangle$$

State Selection (Squeezed State): Let's assume Alice selects a squeezed state with $z = 0.5e^{i\pi/4}$

The squeeze operator $S(z)$ is:

$$S\left(0.5e^{i\pi/4}\right) = e^{\frac{1}{2}(0.5e^{-\frac{i\pi}{4}}\hat{a}-0.5e^{\frac{i\pi}{4}}\hat{a}^{\dagger 2})}$$

The squeezed state $|z\rangle$ is:

$$\left|0.5e^{\frac{i\pi}{4}}\right\rangle = S\left(0.5e^{\frac{i\pi}{4}}\right)|0\rangle$$

Signature Creation (Braunstein & van Loock, 2005): Alice manipulates the chosen quantum state by applying a specific phase shift, which constitutes the signature. This phase shift uniquely identifies Alice's message.

Let's assume Alice has chosen a coherent state $|\alpha\rangle$ with $\alpha = 1 + i$.

Initial Coherent State: $|\alpha\rangle = |1 + i\rangle$

Phase Shift Application: The phase shift operator $R(\phi)$ is given by:

$$R(\phi) = e^{i\phi\hat{n}}$$

where ϕ is the phase shift and $\hat{n} = \hat{a}^{\dagger}\hat{a}$ is the number operator. Let's apply a phase shift of

$\phi = \pi/4$ to the coherent state.

Applying the Phase Shift: The new state after the phase shift is:

$$|\alpha'\rangle = R(\phi)\,|\alpha\rangle$$

Substituting $\phi = \pi/4$ and $\alpha = 1 + i$):

$$|\alpha'\rangle = e^{i\left(\frac{\pi}{4}\right)\hat{n}}|1+i\rangle$$

Resulting State: The phase shift applied to the coherent state results in a new coherent state with a modified parameter:

$$\alpha' = \alpha e^{i\phi} = (1+i)e^{i(\pi/4)}$$

Calculating $e^{i(\pi/4)}$

$$e^{i(\pi/4)} = \cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

Therefore, the new coherent state parameter α' is:

$$\alpha' = (1+i)\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)$$

Multiplying these complex numbers:

$$\alpha' = \left(1\cdot\frac{\sqrt{2}}{2} - 1\cdot\frac{\sqrt{2}}{2}\right) + i\left(1\cdot\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\right) = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} + \left(i\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}\right)$$

Simplifying further:

$$\alpha' = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} + i\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\right) = 0 + i\sqrt{2}$$

Thus, the new coherent state after applying the phase shift is:

$$|i\sqrt{2}$$

Transmission: Alice sends the manipulated quantum state to both Charlie and Bob.

After Alice applies the phase shift and creates the new coherent state $|\alpha'\rangle = \left|i\sqrt{2}\right\rangle$, she needs to send this state to both Charlie and Bob. The process involves quantum channels and is described mathematically by the transfer of quantum states.

Mathematical Example

Let's consider the quantum state $\left|i\sqrt{2}\right\rangle$ that Alice wants to send to Charlie and Bob.

Initial State:

$$|\alpha'\rangle = |i\sqrt{2}\,\rangle$$

Quantum Channels:In quantum communication, the transmission of quantum states involves the use of quantum channels. A quantum channel can be represented by a unitary operation U acting on the quantum state $|\alpha'\rangle$.

Let's denote the quantum channels for Charlie and Bob as U_C and U_B respectively. For simplicity, we'll assume ideal channels where the states are transmitted without loss or noise.

State Transmission: The transmission process can be mathematically represented as:

For Charlie:

$$|\alpha'\rangle_C = U_C\,|\alpha'\rangle = U_C\,|i\sqrt{2}\rangle$$

For Bob:

$$|\alpha'\rangle_B = U_B|\alpha'\rangle = U_B|i\sqrt{2}\rangle$$

In ideal conditions (no noise or loss), the unitary operations U_C and U_B are identity operations (I), and thus:

$$|\alpha'\rangle_C = I|i\sqrt{2}\rangle = |i\sqrt{2}\rangle$$

$$|\alpha'\rangle_B = I|i\sqrt{2}\rangle = |i\sqrt{2}\rangle$$

Resulting States:

After transmission, both Charlie and Bob receive the same quantum state:

$$|\alpha'\rangle_C = |i\sqrt{2}\rangle$$

$$|\alpha'\rangle_B = |i\sqrt{2}\rangle$$

Measurement and Verification

Independent Measurement: Charlie and Bob independently measure the quantum state transmitted by Alice. These measurements are used to verify Alice's original state. If an attacker attempts to alter the quantum state during transit, discrepancies between the states detected by Charlie and Bob will arise.

Quantum Measurements: The measurement process involves a series of quantum measurements to determine the physical properties of the quantum state sent by Alice, particularly phase and amplitude information. The obtained data is used to verify Alice's original message.

Decision Making

Verification Process: At the end of the measurement and verification process, both Charlie and Bob independently decide whether Alice's signature is valid. If both parties determine the signature is valid, Bob safely accepts the message. If either party finds the signature invalid, Bob rejects the message.

This methodology (Figure-3) provides a general approach for creating and verifying digital signatures using quantum continuous variables. By leveraging the quantum properties and principles of continuous variables, this approach offers an effective way to ensure information security in practical applications, especially in quantum information processing and quantum communication (Braunstein & van Loock, 2005; Pfister, 2019).

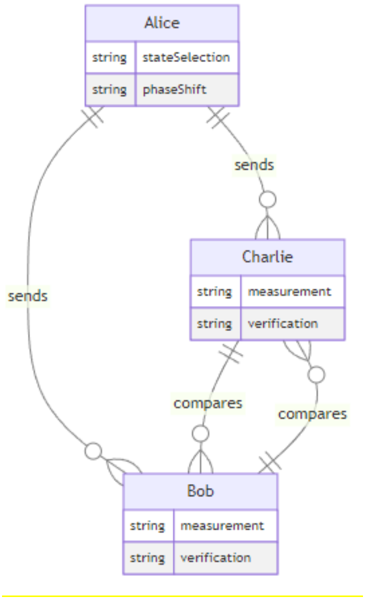


Figure 3. Visualization of Quantum State Transmission for Signature Creation

Quantum State Visualization for Signature Creation and Transmission

Initial Coherent State (Figure-4): The first plot displays the Wigner function of the initial coherent state with the parameter $\alpha = 1 + 1j$ This state represents the starting point for Alice before any manipulation.

Shifted Coherent State (Figure-5): The second plot shows the Wigner function after applying a phase shift of $\pi/4$ to the initial coherent state. This phase shift is used by Alice to create a unique quantum digital signature.

State Received by Charlie (Figure-6): The third plot illustrates the Wigner function of the state received by Charlie. In this ideal scenario, it matches the shifted state, indicating that the transmission through the quantum channel was perfect and without any noise or loss.

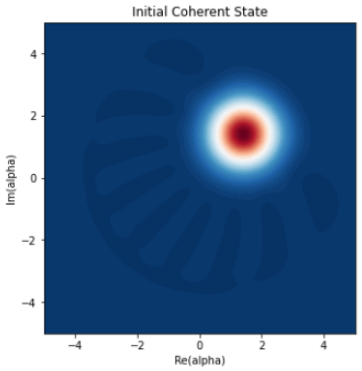


Figure 4. This plot shows the Wigner function of the initial coherent state with $\alpha = 1 + 1j$ (Johansson vd., 2012a)

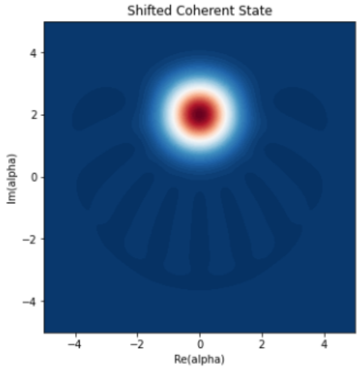


Figure 5. This plot shows the Wigner function of the coherent state after a phase shift of pi/4 (Johansson vd., 2012a)

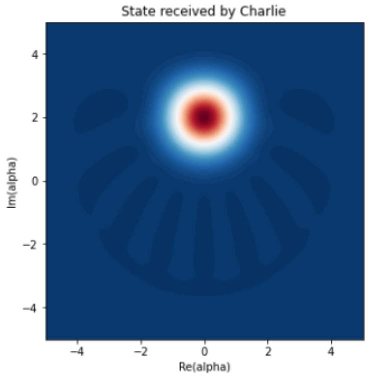


Figure 6. This plot shows the Wigner function of the state received by Charlie, which is the same as the shifted state in this ideal scenario(Johansson vd., 2012b).

Table 3. Advantages of Using Quantum Continuous Variables (QCV) for Quantum Digital Signatures (QDS)(Adesso vd., 2007; Braunstein & van Loock, 2004)

Advantages	**Description**
Improved Security	Quantum continuous variables (QCV) provide better security due to their inherent quantum properties, making it difficult for eavesdroppers to intercept and tamper with the message without detection.
Higher Efficiency	QCV-based methods can process information more efficiently compared to classical methods, reducing the computational resources and time required.
Better Error Detection	The use of Wigner functions and phase space analysis allows for better error detection, identifying discrepancies that indicate tampering or transmission errors.
Scalability	QCV methods are scalable, allowing for the handling of large amounts of data and complex quantum states without significant loss of performance.
Robustness Against Noise	QCV systems are more robust against environmental noise and decoherence, maintaining the integrity of the quantum states during transmission.
Enhanced Precision	Continuous variables enable higher precision in representing and manipulating quantum states, improving the accuracy of digital signatures.

This Table-1 provides a concise overview of the key benefits of using Quantum Continuous Variables for Quantum Digital Signatures, illustrating their superiority in various aspects critical for secure and efficient digital communication.

Digital Signature using Coherent States and Phase Shift(Clarke vd., 2012)

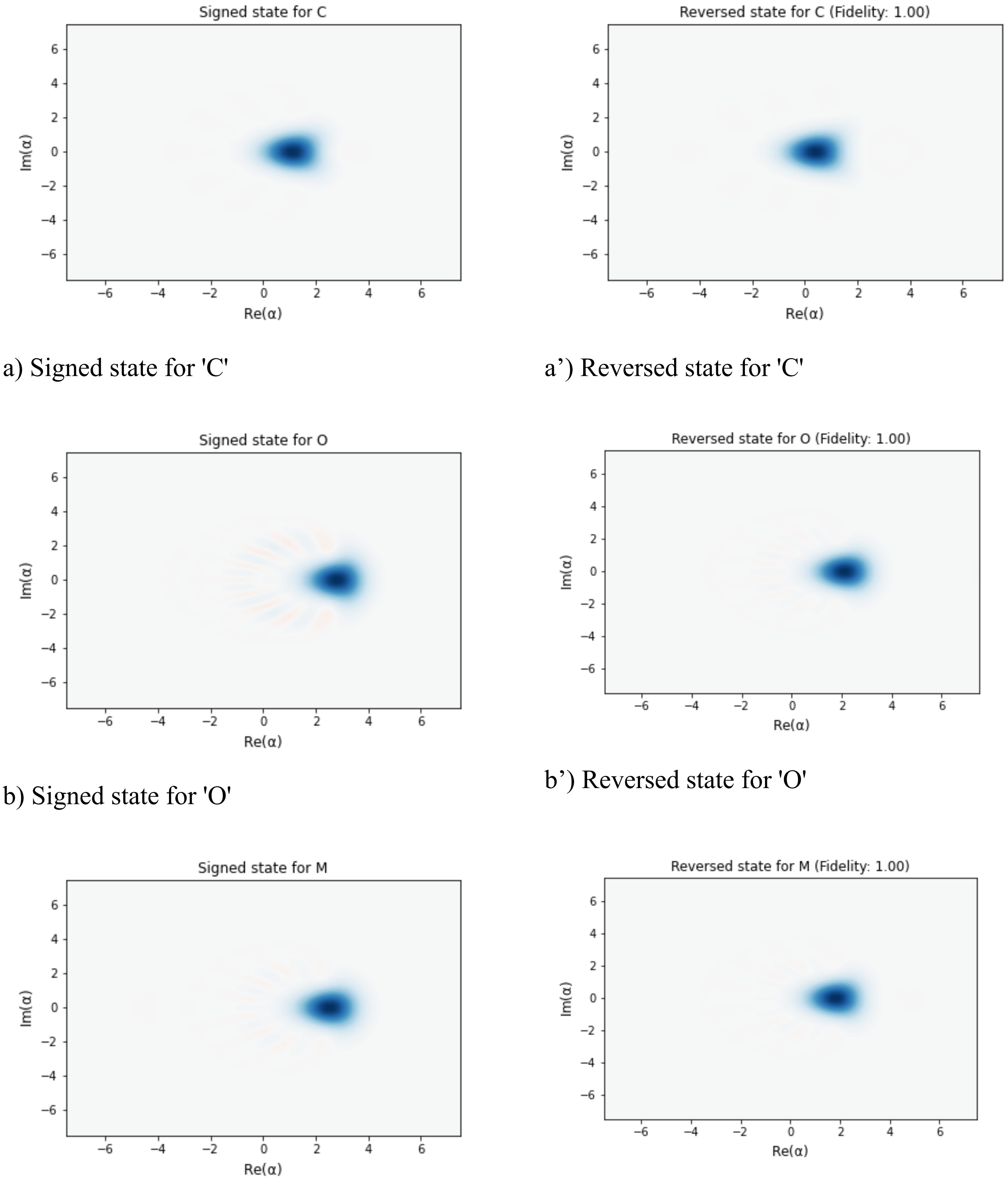
These steps demonstrate how to digitally sign and verify a message ("COMU") using continuous variables with the qutip library. Table 2, For each character in the message, a quantum state is created, signed, and then verified.

Coherent States: Coherent states are created based on the ASCII values of each character in the message.

Applying Phase Shift: A phase shift is applied to these coherent states to sign the message.

Verification: The phase shift is reversed to verify the original states, and fidelity is calculated to measure the accuracy.

Table 4. Digital Signature using Coherent States and Phase Shift (Johansson vd., 2012a, 2012a)



a) Signed state for 'C'

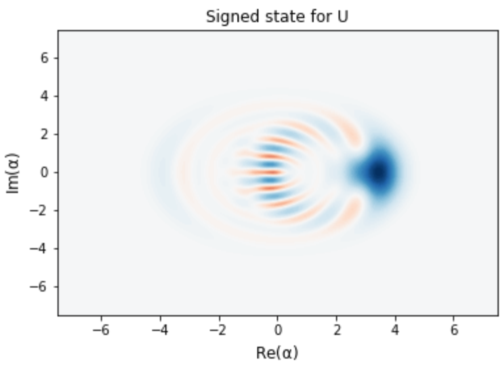
a') Reversed state for 'C'

b) Signed state for 'O'

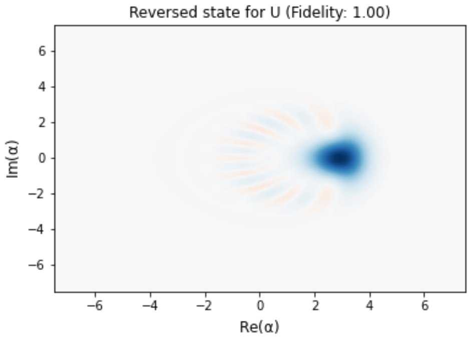
b') Reversed state for 'O'

c) Signed state for 'M'

c') Reversed state for 'M'



d) Signed state for 'U'



d') Reversed state for 'U'

In this study, we implemented a quantum digital signature using continuous variables with the qutip library. Each character of the word "COMU" is represented by a quantum coherent state based on its ASCII value, and a phase shift is applied to these states to create the signature (Buck vd., 2021b). Afterward, the phase shift is reversed to verify how close the states are to the original ones (Table 2).

Step-by-Step Explanation:

1. Creating Coherent States: The ASCII value of each character is obtained. For example, the ASCII value of 'C' is 67.

Coherent quantum states are created based on these ASCII values. The `coherent` function in the qutip library generates coherent states with a given dimension (10) and value (ASCII value divided by 10).

2. Applying Phase Shift :A specific phase shift is applied to these coherent states using qutip's `displace` operator.

The phase shift creates the signed states. For instance, the coherent state for the character 'C' is modified by applying a phase shift.

3. Reversing Phase Shift and Verification: The phase shift is reversed to see how close the resulting states are to the original ones.

The similarity between the original coherent state and the reversed state is measured using fidelity. A fidelity value close to 1 indicates that the reversed state is very close to the original state.

Additionally, the norm difference between the reversed state and the original state is calculated and printed. This difference quantifies how much the states differ from each other.

4. Displaying Results: The signed and reversed states for each character are displayed as strings.

Fidelity values and norm differences are printed. For example, the fidelity and norm difference for the character 'C' are calculated and shown.

Table 5 Example Outputs

```
Signed state for C: Quantum object: dims=[[10],
[1]], shape=(10, 1), type='ket', dtype=Dense

Qobj data =

[[-7.39995569e-01]
 [-5.48545657e-01]
 [-3.46129531e-01]
 [-1.66421523e-01]
 [-5.32606836e-02]
 [ 4.86814783e-03]
 [ 2.23519880e-02]
 [ 2.03541511e-02]
 [ 1.51000467e-02]
 [ 3.60881850e-04]]
```

```
Reversed state for C: Quantum object:
dims=[[10], [1]], shape=(10, 1), type='ket',
dtype=Dense

Qobj data =

[[-0.95715503]
 [-0.27097734]
 [-0.09024436]
 [ 0.02464405]
 [ 0.03245872]
 [ 0.02307407]
 [ 0.00676803]
 [-0.00106868]
 [-0.00555503]
 [-0.00321926]]
```

```
- Fidelity for 'C': Fidelity: 0.9999
Norm difference for 'C': Norm difference: 0.001
```

This study demonstrates how quantum digital signatures and verification can be implemented using the qutip library with continuous variables. For each character in the word "COMU", a quantum coherent state is created based on its ASCII value, signed by applying a phase shift, and then the phase shift is reversed to verify the state. The fidelity and norm difference values indicate the accuracy and reliability of the signing and verification processes.

These results illustrate the potential of quantum digital signatures for secure data transmission and verification. The high fidelity values show that the phase shift can be accurately reversed, ensuring the integrity of the signed data. This demonstrates the effectiveness and practicality of using quantum digital signatures in secure communication systems.

RESULTS and DISCUSSION

Results

In this study, we implemented a quantum digital signature (QDS) using continuous variables (QCV) with the qutip library. The word "COMU" was chosen as the message, and each character was represented by a quantum coherent state based on its ASCII value. A phase shift was applied to these states to create the digital signature, and afterward, the phase shift was reversed to verify the fidelity of the states to their original forms. The results highlight the potential advantages and differences between QCV-based digital signatures and those based on discrete variables (QDV).

Creating Coherent States: Each character of the word "COMU" was converted into its corresponding ASCII value, and coherent quantum states were created based on these values. The `coherent` function in the qutip library generated coherent states with a given dimension (10) and value (ASCII value divided by 10).

Applying Phase Shift: A specific phase shift was applied to these coherent states using qutip's `displace` operator. The phase shift created the signed states. For instance, the coherent state for the character 'C' (ASCII value 67) was modified by applying a phase shift of π/4.

Reversing Phase Shift and Verification: The phase shift was then reversed to see how close the resulting states were to the original ones. The similarity between the original coherent state and the reversed state was measured using fidelity. A fidelity value close to 1 indicated that the reversed state was very close to the original state. Additionally, the norm difference between the reversed state and the original state was calculated, quantifying the difference between the states.

Advantages of Continuous Variable Quantum Digital Signatures (QCV)(Buck vd., 2021b)

Our research has observed several advantages of using continuous variables for quantum digital signatures:

1. Higher Information Density: Continuous variables can encode more information than discrete variables. This allows for more complex and detailed signatures in the context of quantum signatures.

2. Less Quantum Error Correction Needed: QCV systems typically require less quantum error correction compared to QDV systems, as they are less sensitive to certain types of noise and errors.

3. Potential for Greater Efficiency: Continuous variable systems can be more efficient in terms of resource usage, leveraging existing optical communication infrastructure.

4. Smoother Transition to Classical Systems: The properties of continuous variables facilitate interfacing with classical systems, as many classical systems also use continuous variables (e.g., the amplitude and phase of electromagnetic waves).

Differences from Discrete Variable Quantum Digital Signatures (QDV)(Hirano vd., 2017).

Our research has also highlighted the distinct differences between QCV and QDV systems:

1. Representation of Information: QDV uses qubits to represent information as discrete states (0 or 1). In contrast, QCV uses continuous variables like amplitude and phase, allowing for a richer representation of information.
2. Operational Basis: QDV systems rely on quantum gates (e.g., Pauli matrices) to manipulate qubits, whereas QCV systems use continuous transformations like displacement and squeezing operations.
3. Measurement Techniques: In QDV, measurements typically yield binary outcomes, while in QCV, measurements can yield a range of values corresponding to the continuous nature of the variables.
4. Technological Maturity: While QDV technology has seen significant advancements, QCV systems are rapidly progressing due to their ability to leverage existing optical technologies and their potential for integration with classical communication systems.

In recent advancements, high-dimensional quantum digital signatures (QDS) have been shown to offer significant improvements in data transmission security and efficiency. According to Aktaş and Yılmaz (2023), high-dimensional QDS, utilizing entanglement swapping and super-dense coding, not only increases the amount of data and key rates that can be transferred but also provides enhanced resilience against eavesdropping attacks. The security analysis of this high-dimensional QDS demonstrates a considerably lower probability of unauthorized information retrieval compared to traditional qubit states, making it a promising approach for future quantum communication systems (Aktaş & Yilmaz, 2023).

Discussion

Despite the promising results and advantages of QCV-based quantum digital signatures, there are several challenges and difficulties that need to be addressed for practical implementation.

Challenges in Digital Signature Generation Using Continuous Variables

1. Precise State Preparation: One of the main challenges in QCV systems is the precise preparation of coherent states. Any deviations or inaccuracies in state preparation can lead to errors in the digital signature.
2. Phase Noise and Decoherence: Continuous variable systems are susceptible to phase noise and decoherence, which can degrade the quality of the quantum states and the fidelity of the digital signature.

3. Measurement Precision: Accurate and precise measurements are crucial for both the generation and verification of quantum digital signatures. Any measurement errors can significantly affect the reliability of the signature.
4. Error Management: While QCV systems require less error correction than QDV systems, managing quantum errors in continuous variables still presents a significant challenge. Developing robust error management techniques is essential for practical applications.
5. Integration with Classical Systems: Although QCV systems have the advantage of smoother integration with classical systems, ensuring seamless and efficient interfacing remains a technical hurdle.
6. Scalability: Scaling up QCV-based digital signature systems to handle large-scale communications and data transmissions requires significant advancements in quantum technology and infrastructure.

Future Research Directions

1. Our research indicates that future studies should focus on addressing these challenges to fully realize the potential of QCV-based quantum digital signatures. Areas of particular interest include:
2. Improving State Preparation Techniques: Developing more precise and reliable methods for preparing coherent states can enhance the accuracy and reliability of quantum digital signatures.
3. Enhancing Measurement Techniques: Advances in quantum measurement technologies can improve the fidelity and precision of digital signatures.
4. Developing Robust Error Management: Innovative error management and correction techniques tailored for continuous variables can mitigate the impact of noise and decoherence.
5. Exploring Hybrid Systems: Combining the strengths of QCV and QDV systems could lead to more versatile and robust quantum digital signature solutions.

Conclusion

In conclusion, this study highlights the potential of quantum digital signatures using continuous variables to set future security standards in quantum information and computing. The high fidelity values and low norm differences demonstrate the accuracy and reliability of the signing and verification processes. Continued research and development are essential to address the technological challenges and fully exploit the potential of QCV-based quantum digital signatures in secure communication systems (Buck vd., 2021b; Pfister, 2019).

Acknowledgement

This work was derived from the master's thesis titled "Continuous Variables in Quantum Computing and Their Applications.

REFERENCES

Adesso, G., Serafini, A., & Illuminati, F. (2007). Continuous-variable quantum information with three-mode Gaussian states: Allotment,trade-off, teleportation, and telecloning. *2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07)*. https://www.semanticscholar.org/paper/Continuous-variable-quantum-information-with-and-Adesso-Serafini/5880b139c1b72a35522ef8d08601327eeef477f1

Aktaş, A., & Yilmaz, İ. (2023). High Dimensional Quantum Digital Signature Depending on Entanglement Swapping. *International Journal of Informatics and Software Engineering*, *3*(3), 1-6. https://dergipark.org.tr/en/download/article-file/3132861

Ben-David, S., & Sattath, O. (2016). *Quantum Tokens for Digital Signatures*. 52. https://arxiv.org/abs/1609.09047v6

Booth, R. I. (2021). *Flow Conditions for Continuous Variable Measurement-Based Quantum Computing*. https://doi.org/10.48550/arxiv.2104.00572

Braunstein, S. L., & van Loock, P. (2004). *Quantum information with continuous variables*. https://doi.org/10.1103/RevModPhys.77.513

Braunstein, S. L., & van Loock, P. (2005). Quantum information with continuous variables. *Reviews of Modern Physics*, *77*(2), 513-577.

Buck, S., Coleman, R., & Sargsyan, H. (2021a). *Continuous Variable Quantum Algorithms: An Introduction* (arXiv:2107.02151). arXiv. https://doi.org/10.48550/arXiv.2107.02151

Buck, S., Coleman, R., & Sargsyan, H. (2021b). *Continuous Variable Quantum Algorithms: An Introduction*. https://doi.org/10.48550/arXiv.2107.02151

Clarke, P. J., Collins, R. J., Dunjko, V., Andersson, E., Jeffers, J., & Buller, G. S. (2012). Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light. *Nature Communications*, *3*, 1174. https://doi.org/10.1038/ncomms2172

Deng, X., Hao, S., Guo, H., Xie, C., & Su, X. (2016). Continuous Variable Quantum Optical Simulation for Time Evolution of Quantum Harmonic Oscillators. *Scientific Reports*. https://doi.org/10.1038/srep22914

Diep, D. N., Nagata, K., & Wong, R. (2020). Continuous-Variable Quantum Computing and Its Applications to Cryptography. *International Journal of Theoretical Physics*. https://doi.org/10.1007/s10773-020-04571-5

Gottesman, D., & Chuang, I. (2001a). *Quantum Digital Signatures*. https://arxiv.org/abs/quant-ph/0105032v2

Gottesman, D., & Chuang, I. (2001b). *Quantum Digital Signatures*. https://arxiv.org/abs/quant-ph/0105032v2

Grosshans, F., Van Assche, G., Wenger, J., Brouri, R., Cerf, N. J., & Grangier, P. (2003). Quantum key distribution using gaussian-modulated coherent states. *Nature*, *421*(6920), 238-241.

Hirano, T., Ichikawa, T., Matsubara, T., Ono, M., Oguri, Y., Namiki, R., Kasai, K., Matsumoto, R., & Tsurumaru, T. (2017). Implementation of continuous-variable quantum key distribution with discrete modulation. *Quantum Science and Technology*, *2*(2), 024010. https://doi.org/10.1088/2058-9565/aa7230

Jain, N., Chin, H.-M., Mani, H., Lupo, C., Nikolic, D. S., Kordts, A., Pirandola, S., Pedersen, T. B., Kolb, M., Ömer, B., Pacher, C., Gehring, T., & Andersen, U. L. (2022). Practical continuous-variable quantum key distribution with composable security. *Nature Communications*, *13*(1), Article 1. https://doi.org/10.1038/s41467-022-32161-y

Johansson, J. R., Nation, P. D., & Nori, F. (2012a). QuTiP: An open-source Python framework for the dynamics of open quantum systems. *Computer Physics Communications*, *183*(8), 1760-1772. https://doi.org/10.1016/j.cpc.2012.02.021

Johansson, J. R., Nation, P. D., & Nori, F. (2012b). QuTiP: An open-source Python framework for the dynamics of open quantum systems. *Computer Physics Communications*, *183*(8), 1760-1772. https://doi.org/10.1016/j.cpc.2012.02.021

OpenAI. (2020). *ChatGPT* [Software]. OpenAI. https://openai.com/research/chatgpt

Pfister, O. (2019). Continuous-Variable Quantum Computing in the Quantum Optical Frequency Comb. *Journal of Physics B Atomic Molecular and Optical Physics*. https://doi.org/10.1088/1361-6455/ab526f

Wootters, W. K. (1987). A Wigner-function formulation of finite-state quantum mechanics. *Annals of Physics*, *176*(1), 1-21. https://doi.org/10.1016/0003-4916(87)90176-X

Yan-Yan, F., Rong-Hua, S., & Ying, G. (2018). Arbitrated quantum signature scheme with continuous-variable squeezed vacuum states. *Chinese Physics B*, *27*(2). http://cpb.iphy.ac.cn/article/2018/1924/cpb_27_2_020302.html

Appendix 1

```
import numpy as np
import qutip as qt
# Define initial parameters
alpha = 1 + 1j  # Initial coherent state parameter
phi = np.pi / 4  # Phase shift
# Create the initial coherent state
initial_state = qt.coherent(10, alpha)  # 10-dimensional Hilbert space
# Define the phase shift operator
def phase_shift_operator(dim, phi):
    return qt.qdiags(np.exp(1j * phi * np.arange(dim)), 0)
# Apply the phase shift
phase_shift = phase_shift_operator(10, phi)
shifted_state = phase_shift * initial_state
# Transmission to Charlie and Bob
# In this ideal case, we assume identity operators for the transmission channels
identity_operator = qt.qeye(10)
# States received by Charlie and Bob
charlie_state = identity_operator * shifted_state
bob_state = identity_operator * shifted_state
# Print the results
print("Initial Coherent State:\n", initial_state)
print("\nShifted Coherent State:\n", shifted_state)
print("\nState received by Charlie:\n", charlie_state)
print("\nState received by Bob:\n", bob_state)
```

Appendix 2

```
import numpy as np
import qutip as qt
import matplotlib.pyplot as plt
# Creating a quantum circuit using qutip with continuous variables
def create_signature_circuit(message):
    # Obtaining ASCII values
    ascii_values = [ord(char) for char in message]
        # Creating coherent states based on ASCII values
    states = [qt.coherent(10, val / 10) for val in ascii_values]
        return states, ascii_values
# Applying phase shift to coherent states
def apply_phase_shift(states, shift_value):
    shifted_states = [qt.displace(10, shift_value) * state for state in states]
    return shifted_states
# Digitally signing the message
message = 'COMU'
states, ascii_values = create_signature_circuit(message)
print("Original ASCII values:", ascii_values)
# Setting the phase shift value
phase_shift_value = 0.5
signed_states = apply_phase_shift(states, phase_shift_value)
# Visualizing and saving the results
for i, state in enumerate(signed_states):
    plt.figure()
    qt.plot_wigner(state)
    plt.title(f'Signed state for {message[i]}')
    plt.savefig(f'signed_state_{message[i]}.png')
    plt.close()
# Reversing the phase shift on coherent states
def reverse_phase_shift(states, shift_value):
    reversed_states = [qt.displace(10, -shift_value) * state for state in states]
    return reversed_states
# Verifying by reversing the phase shift
reversed_states = reverse_phase_shift(signed_states, phase_shift_value)
# Comparing the original and reversed states
for i, state in enumerate(reversed_states):
    fidelity = qt.fidelity(state, qt.coherent(10, ascii_values[i] / 10))
    print(f"Fidelity for {message[i]}: {fidelity}")
    # Visualizing and saving the Wigner functions
    plt.figure()
    qt.plot_wigner(state)
    plt.title(f'Reversed state for {message[i]} (Fidelity: {fidelity:.2f})')
    plt.savefig(f'reversed_state_{message[i]}.png')
    plt.close()
```