ISSN 1674-1056
http://cpb.iphy.ac.cn
http://iopscience.iop.org/cpb
中国物理 B
Chinese Physics
中国物理
Chinese Physics B

Arbitrated quantum signature scheme with continuous-variable squeezed vacuum states

Yan-Yan Feng(冯艳艳), Rong-Hua Shi(施荣华), Ying Guo(郭迎)
Citation: Chin. Phys. B . 2018, 27(2): 020302. **doi:** 10.1088/1674-1056/27/2/020302

Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Continuous variable quantum key distribution

Yong-Min Li(李永民), Xu-Yang Wang(王旭阳), Zeng-Liang Bai(白增亮), Wen-Yuan Liu(刘文元), Shen-Shen Yang(杨申申), Kun-Chi Peng(彭堃墀)
Chin. Phys. B . 2017, 26(4): 040303. **doi:** 10.1088/1674-1056/26/4/040303

Anonymous voting for multi-dimensional CV quantum system

Rong-Hua Shi(施荣华), Yi Xiao(肖伊), Jin-Jing Shi(石金晶), Ying Guo(郭迎), Moon-Ho Lee
Chin. Phys. B . 2016, 25(6): 060301. **doi:** 10.1088/1674-1056/25/6/060301

Enhanced arbitrated quantum signature scheme using Bell states

Wang Chao, Liu Jian-Wei, Shang Tao
Chin. Phys. B . 2014, 23(6): 060309. **doi:** 10.1088/1674-1056/23/6/060309

Scheme for generating a cluster-type entangled squeezed vacuum state via cavity QED

Wen Jing-Ji, Yeon Kyu-Hwang, Wang Hong-Fu, Zhang Shou
Chin. Phys. B . 2014, 23(4): 040301. **doi:** 10.1088/1674-1056/23/4/040301

Effect of excess noise on continuous variable entanglement sudden death and Gaussian quantum discord

Su Xiao-Long
Chin. Phys. B . 2013, 22(8): 080304. **doi:** 10.1088/1674-1056/22/8/080304

Arbitrated quantum signature scheme with continuous-variable squeezed vacuum states*

Yan-Yan Feng(冯艳艳), Rong-Hua Shi(施荣华), and Ying Guo(郭迎)†

School of Information Science and Engineering, Central South University, Changsha 410083, *China*

(Received 19 October 2017; revised manuscript received 17 November 2017; published online 5 January 2018)

We propose an arbitrated quantum signature (AQS) scheme with continuous variable (CV) squeezed vacuum states, which requires three parties, i.e., the signer Alice, the verifier Bob and the arbitrator Charlie trusted by Alice and Bob, and three phases consisting of the initial phase, the signature phase and the verification phase. We evaluate and compare the original state and the teleported state by using the fidelity and the beam splitter (BS) strategy. The security is ensured by the CV-based quantum key distribution (CV-QKD) and quantum teleportation of squeezed states. Security analyses show that the generated signature can be neither disavowed by the signer and the receiver nor counterfeited by anyone with the shared keys. Furthermore, the scheme can also detect other manners of potential attack although they may be successful. Also, the integrality and authenticity of the transmitted messages can be guaranteed. Compared to the signature scheme of CV-based coherent states, our scheme has better encoding efficiency and performance. It is a potential high-speed quantum signature scheme with high repetition rate and detection efficiency which can be achieved by using the standard off-the-shelf components when compared to the discrete-variable (DV) quantum signature scheme.

Keywords: arbitrated quantum signature, squeezed vacuum state, continuous variable, quantum teleportation

PACS: 03.67.–a, 03.67.Ac, 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/27/2/020302

1. Introduction

A quantum signature is the development or extension of a digital signature. In classical cryptography schemes, the digital signature has a great importance by guaranteeing the proof of the source and the integrity and authenticity of messages. Accordingly, digital signatures have been applied in a wide variety of fields, for example, electronic government affairs, electronic medical and electronic payment. Its security is based on computational complexity. Nevertheless, in theory, any cryptography scheme on account of computational complexity can be compromised. The well-known RSA public key cryptography system has been proven to be quickly cracked via future quantum computers,[1,2] and hence the demand for a more secure cryptography system has become even more urgent. Quantum cryptography can be a powerful solution to this problem and it is the product of the combination of the fundamentals of quantum mechanics and classical cryptography theory. Unlike the mathematics-based classical cryptography, the security of quantum cryptography is guaranteed by the quantum non-cloning theorem and Heisenberg's uncertainty principle, which serve as the internal condition and the external protection, respectively. Designing the secure quantum cryptography protocols based on the special properties of the quantum state is an important research direction of quantum cryptography. Quantum cryptography protocols can be subdivided into QKD, quantum secret sharing (QSS), quantum secure direct communication (QSDC), quantum identity authentication (QIA), quantum signature (QS), quantum coin flipping (QCF), quantum money (QM),[3] quantum private query (QPQ),[4–6] and quantum secure computation (QSC),[7,8] among which the latter four have recently become hot topics and QS is an important foundation of the secure quantum information system and quantum cryptography schemes.

So far, quantum signature schemes have been extensively researched for realizing different purposes, for instance, arbitrated quantum signature (AQS),[9–18] quantum homomorphic signature (QHS),[19,20] quantum blind signature (QBS),[21–24] quantum group signature (QGS),[25–28] quantum proxy signature (QPS),[29] quantum digital signature (QDS),[30–32] and quantum dual signature (QDS).[33,34] Among these schemes, we focus on the AQS scheme. The frame of the AQS scheme was initially raised by Zeng and Keitel[9] by employing three-particle entangled Greenberger–Horne–Zeilinger (GHZ) states. Curty *et al.*[11] investigated and argued that the proposal[9] was not clearly operationally defined and ambiguous. Later Zeng gave a more detailed demonstration and presentation[12] of the previous scheme.[9] Next, instead of GHZ triplet states, Li *et al.*[13] exploited two-particle entangled Bell states to design an AQS scheme, which shows the advantages referring to a better efficiency in transmission and a low complexity in implementation. Zou and Qiu claimed that the above schemes cannot guarantee the disavowal from the receiver and presented an AQS scheme[14] with a public board. Choi *et al.*[15] also pointed out the security problem on AQS schemes. Li *et al.*[16] proposed an AQS protocol replac-

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61379153 and 61572529).

†Corresponding author. E-mail: guoyingcsu@sina.com

© 2018 Chinese Physical Society and IOP Publishing Ltd

ing the quantum one-time pad with the chained CNOT operations. Yang *et al.* put forward an AQS protocol[17] with cluster states, which can achieve an efficiency with 1. Note that these above-mentioned schemes are based on discrete variable (DV) quantum states.

Up to now, quantum signatures can be categorized into two forms, i.e., a DV-based quantum signature and a CV-based quantum signature. The DV-based quantum signature schemes have achieved a great deal of success, which belong to quantum cryptography schemes. Undeniably, the DV-based quantum cryptography schemes have also lots of limitations and difficulties and they are facing more and more challenges.[35] For one thing, the production and the detection of a single photon are tricky and the generation of entangled photon pairs is also very troublesome. The production efficiency of a single photon is very low and it may suffer from the potential photon number splitting attack.[36] Furthermore, the detection of a single photon is confronted with severe limitations. Correspondingly, in practical experiments, weak laser is applied to replace single photon.[37] For another, the communication rate of DV-based quantum cryptography is relatively low. Under such a circumstance, the CV-based quantum cryptography, which uses strong light replacing the single photon or entangled photon pairs, comes out. Compared to the DV-based quantum cryptography, the CV-based quantum cryptography has the strengths[35] referring to simple preparation, superior transmission rate, high detection efficiency and repetition rate and easy implementation in the experiments. In the CV-based quantum communication protocols, the messages are encoded onto the amplitude and phase of CV-based quantum states and can be transmitted with a greater communication rate, such as CV-based quantum teleportation.[38] The required manipulations and measurements can be realized in quantum optics in a simple and efficient way, and the shift amount in the quadrature phase space can be measured by homodyne detection. Therefore, investigations into the CV-based quantum cryptography are of great significance. In the last couple of years, Zeng *et al.*[39] initially researched the CV quantum signature algorithm with CV entangled states in 2007, which is a true quantum signature algorithm using a key-pair, i.e., public verification key and private signature key, and exploits a quantum circuit to compare the original states and the decoded states. It provides a fresh idea and a more efficient method to explore quantum signatures. In 2016, we proposed an AQS scheme based on CV coherent states,[18] which serve as the carrier of the signing messages. Its security is guaranteed by the CV-QKD and the CV-based quantum teleportation, which show a potential high-speed AQS algorithm with high communication rate and detection efficiency. In the same year, Huang *et al.*[40] raised CV-based QIA with a two-mode squeezed vacuum state and coherent state. It is worth mentioning that an AQS scheme is of a better application when compared with a true signature scheme, especially with the reduced requirements on the trustworthiness of the arbitrator.[9]

Motivated by the structure of the AQS with CV-based coherent states, we suggest an AQS scheme with CV-based squeezed vacuum states, which are the simplest squeezed states. The proposed scheme makes the following contributions.

(i) Compared to the above-mentioned DV-based quantum signature schemes, the primary advantage is that the amount of information contained in CV-based quantum states is much larger. Moreover, the CV-based squeezed vacuum states, the carrier of the transmitted messages, are easy to generate and convenient to use. Most importantly, the essential operations, preparation (degenerate parametric process), transmission, manipulation and measurement can be efficiently executed in quantum optics.

(ii) Compared to the existing CV-based quantum signature schemes,[18,39] the proposed AQS scheme is of a better application than a true quantum signature scheme. Additionally, the effect of squeezed states is in principle better than that of coherent states in terms of the encoding efficiency and the communication quality.

(iii) The proposed scheme can be implemented by using sources of an optical parametric oscillator (OPO), beam splitter (BS), amplitude (AM), and phase modulators (PM), which are compatible with standard telecommunication technology.

The rest of this paper is arranged as follows. Section 2 introduces the CV-based quantum signature algorithm with three phases. Section 3 analyzes the security of the proposed CV-based quantum signature scheme. Finally, the discussions and the conclusions are presented in Section 4.

2. CV-based quantum signature algorithm

For a secure quantum signature scheme, there are a few rules[9] to be expected to be accomplished.

i) No disavowals On one hand, the signer cannot disavow the signed message and the yielded signature. On the other hand, the recipient cannot deny the received message and the homologous signature.

ii) No forgeries and no modifications Anyone cannot forge or modify the signed message or the generated signature derived from the sender successfully.

iii) Fixed assignments Each message corresponds to a specified signature.

To simplify the scheme design and the subsequent security analyses, the classical communication is assumed to be performed in the authenticated channel, and the quantum channel from the sender to the recipient is also authenticated. Note that the current error correction and privacy amplification techniques[41] may be employed to realize the authenticated

channels and the former can be achieved by communicating $[\log(1/\varepsilon_{\rm cor})]$ bit messages, where $\varepsilon_{\rm cor}$ is the error rate. If this assumption does not hold, the process of transferring data will suffer from the potential eavesdropping attack, tampering attack, individual attack, collective attack, and coherent attack, among which the latter three attacks are widely studied in CV-QKD. Three participants, i.e., the sender Alice, the recipient Bob and the third party Charlie, are contained in the suggested scheme, which is composed of three phases, i.e., an initializing phase, a signing phase and a verifying phase. As depicted in Fig. 1, in the initializing phase, the secret keys K_a and K_b and the CV-based Einstein–Podolsky–Rosen (CV-EPR) pairs are generated and distributed. For example, K_a and K_b are prepared over the CV-QKD protocol and then separately assigned to Alice and Bob. The CV-EPR pairs can be obtained by coupling two squeezed states in a 50:50 BS. In the signing phase, the signature $|S\rangle$ of the message $|\xi\rangle$ is created by using the appropriate CV-based encryption algorithm with K_a by Alice, who then sends the message-signature pair $(|\xi\rangle, |S\rangle)$ to Bob. In the verifying phase, Bob encrypts the performed phase and amplitude modulation M^b and the received parameters $|\xi\rangle$ and $|S\rangle$ with K_b and gets $|Y^b\rangle$, which is dispatched to Charlie. Next, Charlie designs a verification parameter t for the comparison $|\xi^c\rangle$ with $|\xi^{c'}\rangle$ and then transmits the value of t to Bob who makes a judgement whether the protocol should continue certifying the original message $|\xi\rangle$ and the teleported message $|\xi^{\rm out}\rangle$. The labels I and II in Fig. 1 denote the initial verification for the comparison of $|\xi^c\rangle$ and $|\xi^{c'}\rangle$, and the second verification for the comparison of $|\xi\rangle$ and $|\xi^{\rm out}\rangle$, respectively. Note that the encryption key K_s and the decryption key K_v can be symmetrical or asymmetric. We consider that K_s and K_v are symmetrical and call the possible external attacker Eve. In what follows, we formulate the three phases and the concrete steps of each phase in detail.

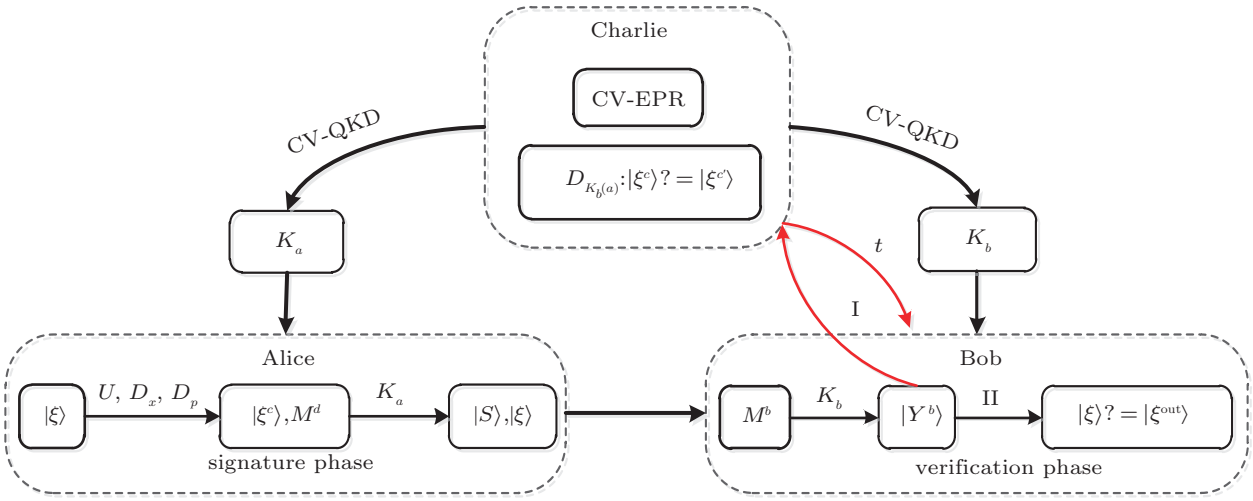


Fig. 1. (color online) The participants and phases of the signature scheme.

2.1. Initial phase

As the first stage to the quantum signature scheme, we state how the secret keys and the CV-based quantum entangled states are created and assigned.

Step 1 Creation and assignment of the secret keys. Alice (Bob) creates the confidential key K_a (K_b) shared with Charlie, which can be achieved in the CV-QKD system[42–46] guaranteeing the perfect secrecy of the keys.

Step 2 Creation and assignment of the CV-based EPR pair. Charlie, a trusted third party, is asked to create the required EPR pair[47] which can be produced by coupling two squeezed beams with squeezing factor r at a 50:50 BS. The generated CV-based EPR pair can be formulated in Heisenberg operators as

$$\hat{x}_a = \frac{1}{\sqrt{2}}(\mathrm{e}^{+r}\hat{x}_a^{(0)} + \mathrm{e}^{-r}\hat{x}_b^{(0)}),$$

$$\hat{p}_a = \frac{1}{\sqrt{2}}(\mathrm{e}^{-r}\hat{p}_a^{(0)} + \mathrm{e}^{+r}\hat{p}_b^{(0)}),$$

$$\hat{x}_b = \frac{1}{\sqrt{2}}(\mathrm{e}^{+r}\hat{x}_a^{(0)} - \mathrm{e}^{-r}\hat{x}_b^{(0)}),$$

$$\hat{p}_b = \frac{1}{\sqrt{2}}(\mathrm{e}^{-r}\hat{p}_a^{(0)} - \mathrm{e}^{+r}\hat{p}_b^{(0)}), \quad (1)$$

where the superscript (0) represents the initial vacuum modes and the subscripts 'a' and 'b' are in one-to-one correspondence with the participants Alice and Bob. Under the condition $r \to \infty$, the eigenstates of the EPR pair are $\hat{p}_a + \hat{p}_b = 0$ and $\hat{x}_a - \hat{x}_b = 0$. Note that the process mentioned above can be accomplished via an authenticated manner.

2.2. Signature phase

As the critical stage to the quantum signature scheme, we elaborate on how to create the signature of the transmitted message. This phase can ensure the integrality and reliability

of the message and deter the possible disavowal attacks from Alice.

Step 1 Alice prepares a sequence $|\xi\rangle$ of squeezed vacuum states (simplest squeezed states) which carries the message to be signed. Assume that $|\xi\rangle$ consists of n squeezed vacuum states, i.e.,

$$|\xi\rangle = \{|\xi_1\rangle, |\xi_2\rangle, \ldots, |\xi_k\rangle, \ldots, |\xi_n\rangle\}, \tag{2}$$

where $|\xi_k\rangle \in \{|0\rangle, |\mathrm{i}0\rangle, |-0\rangle, |-\mathrm{i}0\rangle\}$ $(k = 1,2,\ldots,n)$ represents a squeezed vacuum state. Note that

$$\begin{aligned} m &= (m_1, m_2) \\ &= \{(m_1^1, m_2^1), (m_1^2, m_2^2), \ldots, (m_1^k, m_2^k), \ldots, (m_1^n, m_2^n)\}, \end{aligned} \tag{3}$$

is a corresponding $2n$-length binary-valued classical information string, where $m_1 = \{m_1^1, m_1^2, \ldots, m_1^k, \ldots, m_1^n\}$ and $m_2 = \{m_2^1, m_2^2, \ldots, m_2^k, \ldots, m_2^n\}$ with $m_1^k, m_2^k \in \{0,1\}$. As presented in two columns on the left of Table 1, m is encoded onto the squeezed vacuum states in a specific way. Also, $|\xi_k\rangle$ is of the form

$$|\xi_k\rangle = S(\xi_k)|0\rangle, \tag{4}$$

where $|0\rangle$ is the vacuum state and

$$S(\xi_k) = \exp\left[(\xi_k^* \hat{a}^2 - \xi_k \hat{a}^{\dagger 2})/2\right]$$

is a squeezing operator satisfying $S^{-1}(\xi_k) = S^{\dagger}(\xi_k) = S(-\xi_k)$. $\hat{a}$ and $\hat{a}^{\dagger}$ are separately the annihilation and creation operators. $\xi_k = r\mathrm{e}^{\mathrm{i}\theta_k}$ is a complex squeezing parameter with $r = |\xi|$. Figure 2 shows the squeezed vacuum state $|\xi\rangle$ along the quadrature x derived from vacuum state $|0\rangle$ in the phase space presentation.

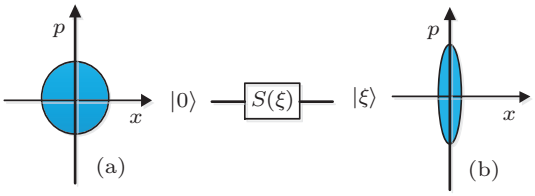


Fig. 2. (color online) The phase space presentation of the squeezed vacuum state $|\xi\rangle$ (b) along the quadrature x derived from the vacuum state $|0\rangle$ (a).

Step 2 Alice applies a unitary phase operator $U = \exp(\mathrm{i}\pi\hat{a}^{\dagger}\hat{a}/2)$, which performs a phase angle transformation $\theta \in \{0, \pi/2, \pi, 3\pi/2\}$ on $|\xi\rangle$, to obtain a confidential quantum state $|\xi^c\rangle$,

$$\begin{aligned} |\xi^c\rangle = U|\xi\rangle &= \exp\{[r(\mathrm{e}^{-\mathrm{i}\theta}\hat{a}^2 - \mathrm{e}^{\mathrm{i}\theta}\hat{a}^{\dagger 2}) + \mathrm{i}\pi\hat{a}^{\dagger}\hat{a}]/2\}|0\rangle \\ &= \{|\xi_1^c\rangle, |\xi_2^c\rangle, \ldots, |\xi_k^c\rangle, \ldots, |\xi_n^c\rangle\}, \end{aligned} \tag{5}$$

where

$$\begin{aligned} |\xi_k^c\rangle &= U|\xi_k\rangle \\ &= \exp\{[r(\mathrm{e}^{-\mathrm{i}\theta_k}\hat{a}^2 - \mathrm{e}^{\mathrm{i}\theta_k}\hat{a}^{\dagger 2}) + \mathrm{i}\pi\hat{a}^{\dagger}\hat{a}]/2\}|0\rangle, \end{aligned} \tag{6}$$

where θ_k is the k_{th} transformation phase angle. We stipulate that $\theta = 0$ or $\theta = \pi/2$ means encoding bit 1 and that $\theta = \pi$ or $\theta = 3\pi/2$ means bit 0. $\theta = 0(\pi/2)$ indicates bit 1 of generation basis $X(P)$ and $\theta = \pi(3\pi/2)$ represents bit 0 of generation basis $X(P)$, as listed in two columns on the right of Table 1.

Table 1. Encoding and phase angle transformation process.

(m_1^k, m_2^k)	$\lvert\xi_k\rangle$	θ	Generation basis (bit)
00	$\lvert 0\rangle$	0	$X(1)$
01	$\lvert \mathrm{i}0\rangle$	$\pi/2$	$P(1)$
10	$\lvert -0\rangle$	π	$X(0)$
11	$\lvert -i0\rangle$	$3\pi/2$	$P(0)$

The variances of a vacuum state are given by

$$\langle(\Delta\hat{x})^2\rangle_{\mathrm{vac}} = \langle(\Delta\hat{p})^2\rangle_{\mathrm{vac}} = 1/4$$

with the canonical communication relation $[\hat{x}, \hat{p}] = \mathrm{i}/2$ $(\hbar = 1/2)$. A squeezed vacuum state is formulated as such a state with reduced variance from the vacuum variance in one quadrature at the expense of increased variance in the other, i.e., $\langle(\Delta\hat{x})^2\rangle < 1/4 < \langle(\Delta\hat{p})^2\rangle$.[38,48] The relationship $\langle(\Delta\hat{x})^2\rangle\langle(\Delta\hat{p})^2\rangle = 1/16$ is satisfied, meaning that the state is the minimum uncertainty state. Taking into account some inevitable losses in real experiments, we acquire that the squeezed states are not pure, but mixed states. The mixed squeezed vacuum state is considered to be a squeezed thermal state. If the x quadrature is squeezed, then the corresponding variances can be given by

$$\begin{aligned} \sigma_{\mathrm{in}}^x &= \langle(\Delta\hat{x}_{\mathrm{in}})^2\rangle = \mathrm{e}^{-2r}[\coth(\beta/2)]/4, \\ \sigma_{\mathrm{in}}^p &= \langle(\Delta\hat{p}_{\mathrm{in}})^2\rangle = \mathrm{e}^{+2r}[\coth(\beta/2)]/4, \end{aligned} \tag{7}$$

where $[\coth(\beta/2)]/4$ denotes the variance of an initial thermal state and β is the inverse temperature $1/2k_{\mathrm{B}}T$ with k_{B} being the Boltzmann constant and T is the temperature. Such a squeezed thermal state is no longer the minimum uncertainty state, holding the inequality $\sigma_{\mathrm{in}}^x \sigma_{\mathrm{in}}^p > 1/16$, as shown in Fig. 3.

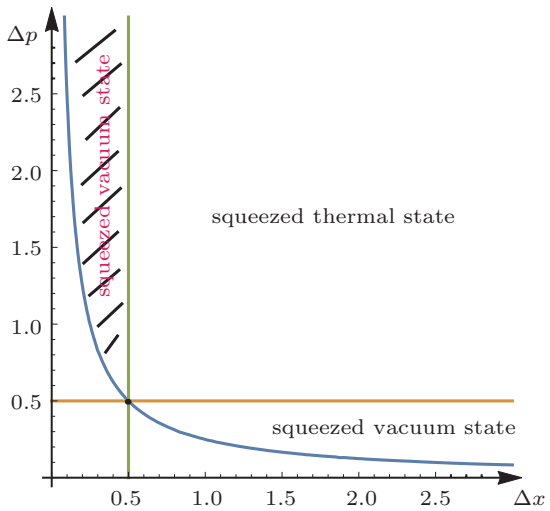


Fig. 3. (color online) The relationship $\langle(\Delta\hat{x})^2\rangle\langle(\Delta\hat{p})^2\rangle = 1/16$. The squeezed vacuum states with $\langle(\Delta\hat{x})^2\rangle < 1/4 < \langle(\Delta\hat{p})^2\rangle$ denoted by the shaded part which is the target area of our study or $\langle(\Delta\hat{p})^2\rangle < 1/4 < \langle(\Delta\hat{x})^2\rangle$ and the squeezed thermal states with $\sigma_{\mathrm{in}}^x \sigma_{\mathrm{in}}^p > 1/16$.

Generally, the Gaussian state can be fully characterized by parameters r, β, angle θ in the coordinates, and the displacement α_0. Setting $\theta = 0$ and $\alpha_0 = 0$ we perform the quantum teleportation of the squeezed vacuum state due to the fidelity as a criteria independent on θ and α_0. The Wigner function[49] of the squeezed thermal state is expressed as

$$W(x,p) = \frac{1}{2\pi\sqrt{\sigma_{\rm in}^x}\sqrt{\sigma_{\rm in}^p}} \times \exp\left[-\left(\frac{1}{2\sigma_{\rm in}^x}x^2 + \frac{1}{\sigma_{\rm in}^p}p^2\right)\right], \quad (8)$$

where x and p serve as the coordinate axes in the phase space. The Wigner function of a vacuum state with $r = 0$ and $\beta \to \infty$ is illustrated in Fig. 4. Note that the squeezed thermal states involve the states whose squeezed variances are larger than the vacuum variance, i.e., $\sigma_{\rm in}^x \geqslant 1/4$. In this paper, we consider the squeezed vacuum state having the squeezed variance $\sigma_{\rm in}^x < 1/4$ and the corresponding quantum teleportation technology.

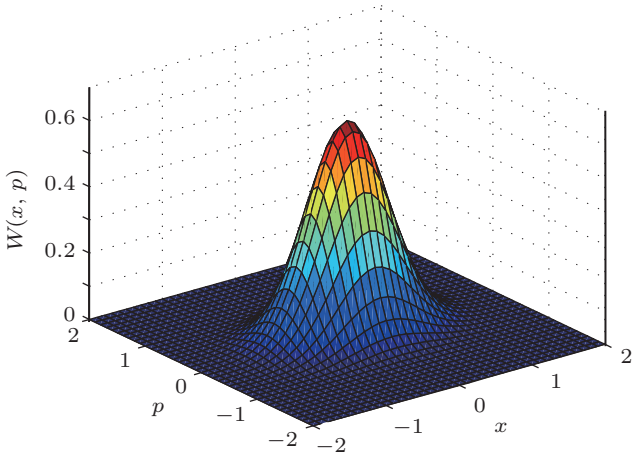


Fig. 4. (color online) The Wigner function for a vacuum state with $r = 0$ and $\beta \to \infty$.

Step 3 Following the CV-based quantum teleportation for a squeezed vacuum state,[38] Alice firstly takes the squeezed vacuum state $|\xi_k\rangle$ and her auxiliary mode a as the incident modes into a balanced 50:50 BS. Afterwards, Alice performs a CV-based "Bell-state" measurement for x and p quadratures by exploiting two balanced homodyne detectors D_x and D_p (x for one beam and p for the other), which consist of the corresponding two local oscillators LO_x and LO_p, resulting in the quadratures $\hat{x}_k^d$ and $\hat{p}_k^d$. We can obtain the output result $M_k^d = \{x_k^d, p_k^d\}$ of the measurement for $(\hat{x}_k^d, \hat{p}_k^d)$. Accordingly, the set M^d is written as

$$M^d = \{M_1^d, M_2^d, \ldots, M_k^d, \ldots, M_n^d\}, \quad (9)$$

and then (it is) teleported to Bob via an auxiliary classical channel.

Step 4 Alice generates the unique quantum signature $|S\rangle$ for $|\xi\rangle$ by encrypting the parameters M^d and $|\xi^c\rangle$ using an appropriate quantum encryption algorithm with K_a as follows:

$$|S\rangle = K_a(M^d, |\xi^c\rangle). \quad (10)$$

Equation (10) plays an important role in ensuring the security of the signature, which includes two aspects. Firstly, the dishonest and hostile participants cannot falsify Alice's signature. Secondly, Alice herself cannot deny her completed signature. To be specific, taking into account the confidentiality of the key K_a shared by Alice and Charlie, we infer that Alice cannot disavow the completed signature in the face of Charlie and Bob successfully and that Bob and the possible attacker cannot counterfeit the signature easily. We note that equation (5) reveals that $|\xi^c\rangle$ is obtained by encrypting the message $|\xi\rangle$, and thus $|S\rangle$ has a connection with $|\xi\rangle$.

Step 5 Alice sends $(|\xi\rangle, |S\rangle)$ to Bob.

2.3. Verification phase

As the last stage to the quantum signature scheme, the purpose is to verify the validity of the signature $|S\rangle$. After receiving the message-signature pair $(|\xi\rangle, |S\rangle)$, Bob is capable of verifying the signature and confirming the authenticity and integrity of the message. Notably, Charlie is required to participate in this phase to assist the verification in that Bob has no access to Alice's key K_a. This phase is composed of the following steps.

Step 1 Due to the existence of entanglement between the modes a and b, Alice's measurement collapses the transmitted message onto mode b. According to the classical result M_k^d from Alice, Bob carries out a phase-space displacement on the mode b, which comprises two parts. To begin with, Bob executes the amplitude and phase modulations M_k^x and M_k^p which translate classical results into complex values. Next, Bob combines the modulated beam with the mode b at a highly reflecting BS (99:1) coherently in the experiment. We describe Bob's measurement set M^b as follows:

$$M^b = \{M_1^b, M_2^b, \ldots, M_k^b, \ldots, M_n^b\}, \quad (11)$$

where $M_k^b = \{M_k^x, M_k^p\}$. Subsequently, Bob encrypts M^b, $|S\rangle$ and $|\xi\rangle$ with K_b to obtain $|Y^b\rangle$

$$|Y^b\rangle = K_b(M^b, |S\rangle, |\xi\rangle), \quad (12)$$

and ultimately transmits $|Y^b\rangle$ to Charlie.

Step 2 After receiving $|Y^b\rangle$ from Bob, Charlie decrypts $|Y^b\rangle$ with K_b to obtain M^b, $|S\rangle$, and $|\xi\rangle$. Then, she decrypts $|S\rangle$ using K_a to gain M^d and $|\xi^{c'}\rangle$. Akin to Ref. [18], Charlie defines a verification parameter t for the comparison of $|\xi^c\rangle$ and $|\xi^{c'}\rangle$ as follows:

$$t = \begin{cases} 0 & \text{if } |\xi^{c'}\rangle \neq |\xi^c\rangle = U|\xi\rangle, \\ 1 & \text{if } |\xi^{c'}\rangle = |\xi^c\rangle = U|\xi\rangle, \end{cases} \quad (13)$$

where $|\xi^c\rangle$ and $|\xi^{c'}\rangle$ separately derive from $|\xi\rangle$ and $|S\rangle$. Afterwards, Charlie generates $|Y^{tb}\rangle$ by encrypting the parameters M^d, M^b, $|S\rangle$ and t with K_b, i.e.,

$$|Y^{tb}\rangle = K_b(M^d, M^b, |S\rangle, t), \quad (14)$$

and sends it to Bob.

Step 3 Bob decrypts the received $|Y^{tb}\rangle$ via K_b and obtains M^d, M^b, $|S\rangle$, and t. Following the result of t, Bob verifies the validity of Alice's signature $|S\rangle$ initially. If $t=0$, the signature $|S\rangle$ is considered to be invalid. We infer that it has been counterfeited and Bob rejects it directly. If $t=1$, for one thing, this case only shows that the signed message is derived from Alice. Bob must keep on with the further verification for comparing the transmitted message $|\xi\rangle$ and the teleported message

$$|\xi^{\text{out}}\rangle=\{|\xi_1^{\text{out}}\rangle,|\xi_2^{\text{out}}\rangle,\ldots,|\xi_k^{\text{out}}\rangle,\ldots,|\xi_n^{\text{out}}\rangle\}.$$

For another thing, the signature may have been fabricated by the attacker based on Eq. (10). Therefore, to demonstrate that the signature is completely correct, the comparison of $|\xi\rangle$ and $|\xi^{\text{out}}\rangle$ must be performed. If they are equal, Bob regards $|S\rangle$ as the valid signature for $|\xi\rangle$ and accepts the message-signature pair $(|\xi\rangle,|S\rangle)$. Otherwise, he abandons it.

Step 4 In the case $t=1$, omitting the losses, we formulate the variances σ_{out}^x and σ_{out}^p [38,50] of the teleported state as follows:

$$\begin{aligned}\sigma_{\text{out}}^x&=g_x^2\sigma_{\text{in}}^x+\frac{\mathrm{e}^{-2r_-}(1+g_x)^2}{8}+\frac{\mathrm{e}^{+2r_+}(1-g_x)^2}{8},\\ \sigma_{\text{out}}^p&=g_p^2\sigma_{\text{in}}^p+\frac{\mathrm{e}^{-2r_-}(1+g_p)^2}{8}+\frac{\mathrm{e}^{+2r_+}(1-g_p)^2}{8},\end{aligned}\tag{15}$$

where r_- and r_+ are the respective squeezing and anti-squeezing parameters for squeezed states, which are exploited to create the EPR beams. g_x and g_p are rightly normalized gains for classical channels with $g_x=\langle\hat{x}_{\text{out}}\rangle/\langle\hat{x}_{\text{in}}\rangle$ and $g_p=\langle\hat{p}_{\text{out}}\rangle/\langle\hat{p}_{\text{in}}\rangle$. We investigate that the squeezed variances for the squeezed vacuum state are suitably transferred to indirectly accomplish the required comparison. Considering $g_x=g_p=g=1$, we rewrite Eq. (15) in a compact form as

$$\begin{aligned}\sigma_{\text{out}}^x&=\sigma_{\text{in}}^x+\frac{\mathrm{e}^{-2r_-}}{2},\\ \sigma_{\text{out}}^p&=\sigma_{\text{in}}^p+\frac{\mathrm{e}^{-2r_-}}{2}.\end{aligned}\tag{16}$$

For $r_-\to+\infty$, $\sigma_{\text{out}}^x=\sigma_{\text{in}}^x$, and $\sigma_{\text{out}}^p=\sigma_{\text{in}}^p$ can be obtained, which indicates that $|\xi\rangle$ is transferred perfectly with $|\xi\rangle=|\xi^{\text{out}}\rangle$. Then Bob can determine the validity of $|S\rangle$. If r_- is a finite value with $r_-=r_+=r$ and $\beta\to\infty$, equation (16) becomes

$$\sigma_{\text{out}}^x=\frac{3\,\mathrm{e}^{-2r}}{4},\quad \sigma_{\text{out}}^p=\frac{3\,\mathrm{e}^{+2r}}{4}.\tag{17}$$

To implement quantum teleportation[38] in real experiments, the following inequalities should be satisfied

$$\begin{aligned}(\sigma_{\text{out}}^x)_{\text{sq}}&<(\sigma_{\text{out}}^x)_{\text{vac}},\\ (\sigma_{\text{out}}^p)_{\text{sq}}&>(\sigma_{\text{out}}^p)_{\text{vac}}.\end{aligned}\tag{18}$$

Taking x quadrature as an example, we demand $\sigma_{\text{out}}^x=(3\,\mathrm{e}^{-2r})/4<1/4$, i.e., $\mathrm{e}^{-2r}<1/3$. Similarly, the inequality $\sigma_{\text{out}}^p>1/4$ holds. Therefore, the squeezed variances of the squeezed vacuum state are teleported successfully and Bob receives the transmitted squeezed vacuum state $|\xi\rangle$ followed by the signature $|S\rangle$. Otherwise, Bob quits.

The above-described procedure is the application of the quantum teleportation with the CV-based squeezed vacuum states which is generally evaluated by calculating fidelity F denoting the overlap of the input and output states. $F=0$ means that the teleported state is orthogonal to the input state and $F=1$ means that $|\xi^{\text{out}}\rangle=|\xi\rangle$ holds. For pure state and mixed state, the expression of the fidelity is different. If the input state $|\xi\rangle$ is a pure state, the fidelity is given by

$$F=\langle\xi_{\text{in}}|\hat{\rho}_{\text{out}}|\xi_{\text{in}}\rangle=|\langle\xi^{\text{out}}|\xi\rangle|^2\tag{19}$$

with the output state $\hat{\rho}_{\text{out}}=|\xi^{\text{out}}\rangle$. For $|\xi^{\text{out}}\rangle=|\xi\rangle$, the fidelity reaches 1, i.e., $F=1$.

If an input state is a mixed state (the mixed squeezed vacuum state is regarded as a squeezed thermal state), the fidelity is expressed as

$$F=\left\{\mathrm{Tr}\left[\left(\sqrt{\hat{\rho}_{\text{in}}}\hat{\rho}_{\text{out}}\sqrt{\hat{\rho}_{\text{in}}}\right)^{1/2}\right]\right\}^2,$$

which similarly shows the match of the states $\hat{\rho}_{\text{in}}$ and $\hat{\rho}_{\text{out}}$. The higher the fidelity F is, the better the receiver reconstructs. In real experiments, the fidelity for the mixed squeezed vacuum states in Eq. (19) can be calculated as[51]

$$F=\frac{2\sinh(\beta_{\text{in}}/2)\sinh(\beta_{\text{out}}/2)}{\sqrt{Y}-1},\tag{20}$$

where Y takes the form

$$\begin{aligned}Y=&\cosh^2(r_{\text{in}}-r_{\text{out}})\cosh^2[(\beta_{\text{in}}+\beta_{\text{out}})/2]\\ &-\sinh^2(r_{\text{in}}-r_{\text{out}})\cosh^2[(\beta_{\text{in}}-\beta_{\text{out}})/2].\end{aligned}\tag{21}$$

We denote the squeezing parameter r_j and the inverse temperature β_j as

$$r_j=\frac{1}{4}\ln\left(\frac{\sigma_j^p}{\sigma_j^x}\right),\quad \beta_j=\ln\left(1+\frac{2}{4\sqrt{\sigma_j^x\sigma_j^p}-1}\right),\tag{22}$$

where $j\in\{\text{in},\text{out}\}$. Accordingly, the fidelity can be calculated with the measured practical variances.

In fact, the comparison of the input squeezed vacuum state $|\xi_k\rangle$ ($|\xi\rangle$) and the received squeezed vacuum state $|\xi_k^{\text{out}}\rangle$ ($|\xi^{\text{out}}\rangle$) can be realized with BSs and photon detectors with a high success probability in experiments.[52] Given two squeezed vacuum states $|\xi_{\text{in}}\rangle$ and $|\xi_{\text{out}}\rangle$ with $|\xi_{\text{in}}\rangle=s_{\text{in}}\exp(\xi_{\text{in}}\hat{c}_{\text{in}}^{\dagger 2})|0\rangle$ and $|\xi_{\text{out}}\rangle=s_{\text{out}}\exp(\xi_{\text{out}}\hat{d}_{\text{in}}^{\dagger 2})|0\rangle$, where s_{in} and s_{out} are the normalization constants. As shown in Fig. 5, if two creation operators $\hat{c}_{\text{in}}^{\dagger}$ and $\hat{d}_{\text{in}}^{\dagger}$ are incident on a balanced BS, the yielding output operators $\hat{c}_{\text{out}}^{\dagger}$ and $\hat{d}_{\text{out}}^{\dagger}$ are

$$\hat{c}_{\text{out}}^{\dagger}=\frac{1}{\sqrt{2}}(\hat{c}_{\text{in}}^{\dagger}+\hat{d}_{\text{in}}^{\dagger}),\quad \hat{d}_{\text{out}}^{\dagger}=\frac{1}{\sqrt{2}}(\hat{c}_{\text{in}}^{\dagger}-\hat{d}_{\text{in}}^{\dagger}).\tag{23}$$

Then, a BS transforms the two squeezed vacuum states $|\xi_{\text{in}}\rangle$ and $|\xi_{\text{out}}\rangle$. We obtain

$$|\xi_{\rm in}\rangle\otimes|\xi_{\rm out}\rangle = s_{\rm in}s_{\rm out}\exp(\xi_{\rm in}\hat{c}_{\rm in}^{\dagger 2}+\xi_{\rm out}\hat{d}_{\rm in}^{\dagger 2})|0\rangle = s_{\rm in}s_{\rm out}\exp\left\{\frac{1}{2}[\xi_{\rm in}(\hat{c}_{\rm out}^{\dagger}+\hat{d}_{\rm out}^{\dagger})^2+\xi_{\rm out}(\hat{c}_{\rm out}^{\dagger}-\hat{d}_{\rm out}^{\dagger})^2]\right\}|0\rangle$$
$$= s_{\rm in}s_{\rm out}\exp\left[\frac{1}{2}(\xi_{\rm in}+\xi_{\rm out})(\hat{c}_{\rm out}^{\dagger 2}+\hat{d}_{\rm out}^{\dagger 2})+(\xi_{\rm in}-\xi_{\rm out})\hat{c}_{\rm out}^{\dagger}\hat{d}_{\rm out}^{\dagger}\right]|0\rangle. \quad (24)$$

For $\xi_{\rm in}=\xi_{\rm out}$, we find that both output modes contain only even numbers of photons. If an odd number of photons are detected in either of the outputs with perfect photon detectors, it signifies that $\xi_{\rm in}\neq\xi_{\rm out}$. Correspondingly, if an even number of photons are detected, it signifies that $\xi_{\rm in}\neq-\xi_{\rm out}$. In experiments, counting photons is rather cumbersome,[52] however photon chopping implemented by using a time resolved multi-port splitter may be possible for small photon numbers. Therefore, the two squeezed vacuum states can be compared by judging the relations of the squeezing factors $\xi_{\rm in}$ and $\xi_{\rm out}$ with detecting the number of photons.

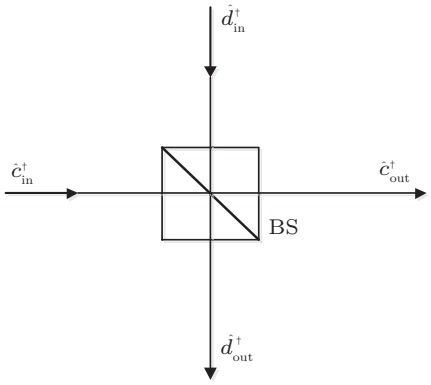


Fig. 5. The BS couples the two input operators of $\hat{c}_{\rm in}^{\dagger}$ and $\hat{d}_{\rm in}^{\dagger}$ in a linear way.

3. Security analyses

To begin with, we recall that Charlie serves as an important role in the proposed AQS scheme. In the initial stage, Charlie creates the CV-based EPR entangled state and the secret key K_a (K_b) shared with Alice (Bob). In the verification stage, Charlie defines the verification parameter t for comparing the secret quantum states $|\xi^c\rangle$ and $|\xi^{c'}\rangle$. In essence, Charlie plays the genuine role of the arbitrator to resolve the possible disputes between Alice and Bob. Hence, he must be absolutely trustworthy in this scheme. Subsequently, we first make the security analyses on the suggested scheme with respect to the security rules, i.e, impossibility of disavowals, impossibility of forgeries and impossibility of repudiations. Furthermore, according to the cryptanalysis in Ref. [53], we analyze the security of the proposed AQS scheme against Bob's forgery and Alice's disavowal under the circumstance of a known message attack.

3.1. Security against disavowals

From the expression in Eq. (10), we see that Alice generates the signature $|S\rangle$ of the message $|\xi\rangle$ with the key K_a which is of the essence for the generation of $|S\rangle$. If Alice disavows her accomplished signature giving rise to the disputes with Bob, it can be easily detected and then solved by timely transmitting the signature $|S\rangle$ to Charlie. From the key K_a point of view, if $|S\rangle$ contains K_a, the signature must have been created by Alice, otherwise, we infer that the signature $|S\rangle$ has been forged by the internal dishonest Bob or the external attacker Eve. Furthermore, we can quantify the possibility of disavowal. Note that Alice may disavow or accept the generated signature $|S\rangle$. The probability of disavowal or acceptance from Alice is respective $1/2$. We call "disavowal" and "acceptance" as dichotomous variables. It conforms to the definition of the Binomial distribution. We assume that k denotes the amount of disavowed signature from n amount of the target signature. So the probability of disavowal about the signature from Alice is

$$P_{\rm disavowal}(k) = \binom{n}{k}\left(\frac{1}{2}\right)^k\left(\frac{1}{2}\right)^{n-k}, \quad (25)$$

where $\binom{n}{k}$ is the Binomial coefficient and can be written as

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \quad (26)$$

Assume that $P_{\rm threshold}$ is the appropriate threshold of $P_{\rm disavowal}(k)$. As depicted in Fig. 6, the success disavowal probability $P_{\rm disavowal}(k)$ is a function of k for the respective $n=50$, $n=100$, and $n=150$, each of which holds a maximum probability value. Also, it becomes smaller with the larger n. Thus, we can figure out that the probability $P_{\rm disavowal}(k)$ can be very small for the large enough n. If the calculated probability $P_{\rm disavowal}(k)$ exceeds $P_{\rm threshold}$, it is regarded as the "disavowal" behavior. Therefore, the proposed AQS scheme can work well against the disavowal attack strategy.

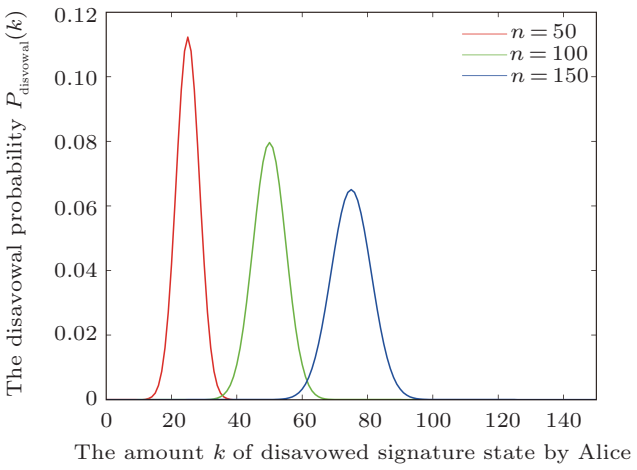


Fig. 6. (color online) The success disavowal probability $P_{\rm disavowal}(k)$ as a function of k for the respective $n=50$, $n=100$, and $n=150$.

3.2. Security against forgeries

For the purpose of their benefit, a dishonest Bob or an external attacker may try to forge Alice's signature. In what follows, we show that any attempt to forge the signature $|S\rangle$ will be absolutely detected.

Assume that Bob is dishonest and (is) in an attempt to forge Alice's signature $|S\rangle$. If he succeeds, he must know the components of $|S\rangle$ including K_a, M_d, and $|\xi^c\rangle$. Nevertheless, obtaining the above ingredients for Bob is impossible. Firstly, K_a is shared by Alice and Charlie and prepared by the CV-QKD with the unconditional security. Bob has no ability to obtain the key K_a, which is the biggest obstacle for successfully forging the signature. Furthermore, we claim that the yielded quantum state $|\xi^c\rangle$ is related to K_a due to the relation of $U|K_a\rangle = \lambda|K_a\rangle$, where λ is the corresponding eigenvalue of the eigenvector K_a.[9] This leads to the unavailability of the correct $|\xi^c\rangle$ without the key K_a, which implies that $t = 0$ will be obtained in the verification phase. Therefore, Charlie can easily detect the forgery strategy from Bob.

The dishonest participant generally has more right than an external attacker. We have analyzed that the forgery strategy from the dishonest Bob is impossible to succeed, and hence the attacker is bound to be unsuccessful in our scheme. This is because there is no information about the keys K_a and K_b via the exposure of the public parameters $|S\rangle$, $|\xi\rangle$, $|Y^b\rangle$, and $|Y^{tb}\rangle$, which are generated by the CV-based quantum cryptography with high security. Even if the attacker achieves K_a and K_b, according to Eq. (10), the forgery of the signature remains impossible due to the additional requirements of $|\xi^c\rangle$ and M^d. The attacker has no access to M^d teleported through a secure classical channel, which is not an expensive resource. Therefore, with the incorrect M^d resulting in the final incorrect recovery of the original message $|\xi\rangle$, we cannot get the relation $|\xi\rangle = |\xi^{\text{out}}\rangle$. That is, the forgery attack from the attacker cannot work. In short, neither the internal dishonest participant nor the external attacker can forge the signature successfully.

3.3. Security against repudiations

From the application's point of view, the scheme should satisfy that the receiver Bob cannot repudiate his receiving of the signature $|S\rangle$ of the message $|\xi\rangle$. Our scheme contains this property. In Step 1 of the verification phase, we assume that Bob transmits $|Y^b\rangle$ to Alice in place of Charlie. Afterwards, Alice generates the new signature $|\tilde{S}\rangle$, i.e.,

$$|\tilde{S}\rangle = K_a(M^d, |\xi^c\rangle, |Y^b\rangle), \tag{27}$$

and then sends it to Charlie. After receiving $|\tilde{S}\rangle$, Charlie transforms $|Y^{tb}\rangle$ in Step 2 of the verification stage as

$$|\tilde{Y}^{tb}\rangle = K_b(M^d, M^b, |\tilde{S}\rangle, t). \tag{28}$$

We see that the new signature $|\tilde{S}\rangle$ contains the keys K_a and K_b. Therefore, following the security analyses against disavowals, if Bob repudiates his receiving of the signature, his action can be found by transmitting $|\tilde{S}\rangle$ to Charlie. Note that the repudiation probability by Bob can also be calculated via the employed method of the disavowal probability by Alice and the same conclusion can be drawn.

3.4. Alice's disavowal

Based on the cryptanalysis in Ref. [53], another disavowal attack strategy by Alice may be successful. For example, when Charlie, sends $|Y^{tb}\rangle = K_b(M^d, M^b, |S\rangle, t)$ to Bob in Step 2 of verification phase, Alice has a chance to modify the signature $|S\rangle$ in terms of phase resulting in the modified signature $|S'\rangle$ that is not a valid signature of $|\xi\rangle$ anymore, which seems to be successful. Meanwhile, since Bob does not hold the secret K_a, he cannot find Alice's modification on $|S\rangle$. Therefore, when a dispute appears, Bob transmits $(|\xi\rangle, |S'\rangle)$ to Charlie. The modified signature will not pass Charlie's verification and Charlie will stand on the side of Alice, believing that Bob forged the signature. Therefore, the proposed AQS scheme cannot deter this attack under non-authenticated channels. Fortunately, no matter whether Charlie judges who disavows or forges the signature, such a kind of communication will be terminated eventually.

3.5. Bob's forgery

In Subsection 3.2, we have demonstrated that Bob's forgery strategy by obtaining the key K_a is impossibly successful. However, based on the cryptanalysis in Ref. [53], another forgery attack strategy by Bob without K_a may be successful. For example, we assume that Bob has a valid message-signature pair $(|\xi\rangle, |S\rangle)$ of Alice, and he performs the so-called CV-based Pauli gates $\bigotimes_{i=1}^{n} P_i$ (P_i is any Pauli operation belonging to $\{I, \hat{X}(x) = \mathrm{e}^{-2\mathrm{i}x\hat{p}}, \hat{Z}(p) = \mathrm{e}^{2\mathrm{i}p\hat{x}}, \hat{X}(x)\hat{Z}(p) = \mathrm{e}^{-2\mathrm{i}x\hat{p}}\hat{Z}(p)\hat{X}(x)\}$) on the squeezed vacuum states in $|\xi\rangle$, and the same operations on the last n quantum states in $|S\rangle$, which is required in the situation where the employed encryption and decryption algorithms are one of the CV-based Pauli gates. The yielding new pair $(|\xi'\rangle, |S'\rangle)$ will be a successful forgery. Hence, Bob can select the most preferred message $|\xi'\rangle_{\text{pr}}$ from at least $4^n - 1$ different forgeries and state that it is derived from Alice. In this situation, Charlie will agree with Bob although Alice is actually aggrieved. Therefore, the proposed AQS scheme cannot deter this attack under the circumstance of the known message attack. Fortunately, no matter whether Charlie judges who disavows or forges the signature, such a kind of communications can be terminated eventually.

4. Discussion and conclusion

In principle, when playing the role of information carrier, squeezed states are better than coherent states. In our scheme, the original binary-valued messages are encoded onto the CV-based squeezed vacuum states, as listed in Table 1. On one

hand, the encoding efficiency has distinct advantages over that in the DV-based signature schemes due to the intrinsic CV-based spectrum. From Table 1, we see that two binary bits can be encoded with a phase transformation, which is more efficient than the quantum state conjugate coding manner in Ref. [18] where only one binary bit can be encoded. We acquire that the length of the corresponding binary-valued classical information string is the respective $2n$ and n for the n squeezed vacuum states and coherent states. On the other hand, the performance of the proposed signature scheme is partially evaluated using fidelity due to the application of the CV-based quantum teleportation. It is demonstrated that the fidelity of quantum teleportation based on squeezed (vacuum) states is higher than that of the quantum teleportation with coherent states.[38,54] Therefore, our scheme has better encoding efficiency and performance. Additionally, as depicted in Fig. 7, the proposed scheme can be achieved in the experiments and the experimental setup of our scheme can be easily obtained due to the achievable CV-based quantum teleportation and CV-QKD.

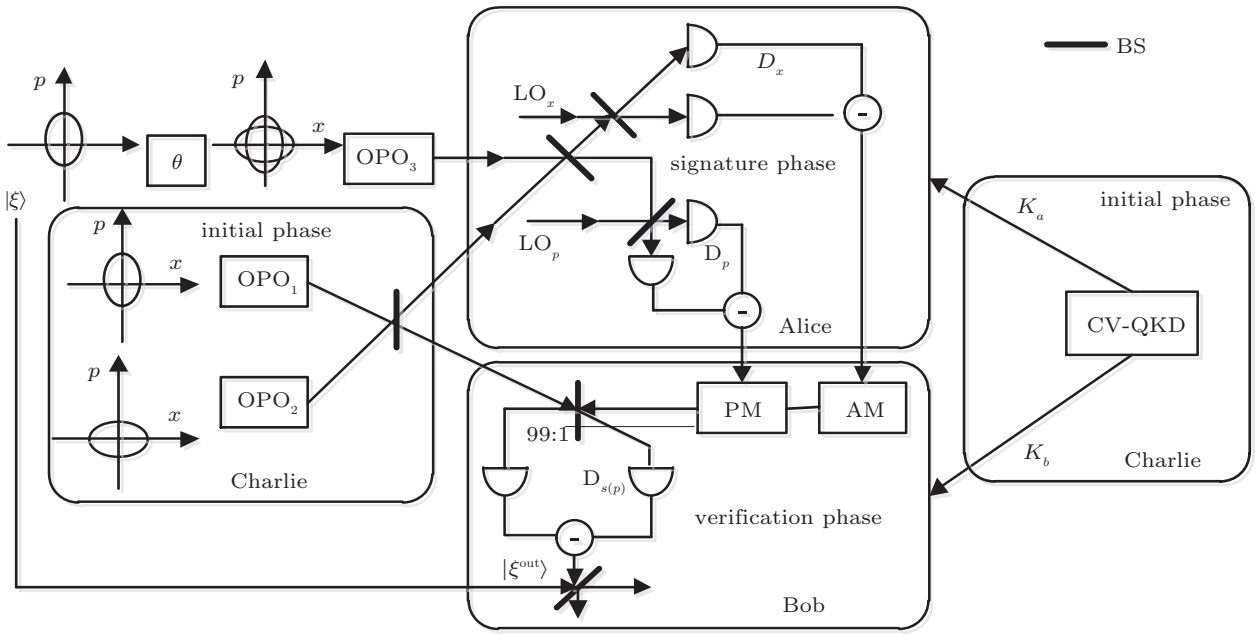


Fig. 7. Experimental setup for the proposed AQS scheme. OPO ($i = 1, 2, 3$): optical parametric oscillator, LO: local oscillator for x and p, D: detector for x and p, BS: 50:50 beam splitter except the marked one 99:1, AM: amplitude modulator, PM: phase modulator.

We have proposed an AQS scheme with CV-based squeezed vacuum states, which requires three participants to jointly complete the initial phase, the signature phase and the verification phase. In the initial phase, the secure keys are prepared and distributed to the legal participants. In the signature phase, the signature is finally generated by employing the unitary phase transformation and the CV-based quantum encryption algorithm. In the verification phase, the validity of the yielded signature is verified via the comparison of the transmitted messages and the recovered messages with the fidelity and the BS technology. The security of our scheme is ensured by the CV-based quantum teleportation and the CV-QKD. Security analyses demonstrate that the proposed scheme can deter the disavowal and forgery attack strategies with the shared keys. However, it is not resistant to Alice's disavowal and Bob's forgery strategies in the circumstance of known message attack, which will be improved in the future study. In addition, the scheme has better coding efficiency and communication performance. Therefore, the proposed AQS scheme may be practical for the general authentication system and the voting mechanism.

References

[1] Nielsen M A and Chuang I L 2000 *Quantum information* (Cambridge: Cambridge University Press)
[2] Wang B, Wu X and Meng F 2017 *J. Comput. Appl. Math.* **313** 185
[3] Amiri R and Arrazola J M 2017 *Phys. Rev. A* **95** 062334
[4] Gao F, Liu B, Huang W and Wen Q Y 2015 *IEEE. J. Sel. Top. Quant.* **21** 98
[5] Wei C Y, Wang T Y and Gao F 2016 *Phys. Rev. A* **93** 042318
[6] Wei C Y, Cai X Q, Liu B, Wang T and Gao F 2017 *IEEE T. Comput.* DOI: 10.1109/TC.2017.2721404
[7] Shi R H, Mu Y, Zhong H and Zhang S 2015 *Phys. Rev. A* **92** 022309
[8] Shi R H, Mu Y, Zhong H, Zhang S and Cui J 2016 *Inform. Sci.* **370–371** 147
[9] Zeng G and Keitel C H 2002 *Phys. Rev. A* **65** 042312
[10] Lee H, Hong C, Kim H, Lim J and Yang H J 2004 *Phys. Lett. A* **321** 295
[11] Curty M and Lütkenhaus N 2008 *Phys. Rev. A* **77** 046301
[12] Zeng G 2008 *Phys. Rev. A* **78** 016301
[13] Li Q, Chan W H and Long D Y 2009 *Phys. Rev. A* **79** 054307
[14] Zou X and Qiu D 2010 *Phys. Rev. A* **82** 042325
[15] Choi J W, Chang K Y and Hong D 2011 *Phys. Rev. A* **84** 062330
[16] Li F G and Shi J H 2015 *Quantum Inf. Process.* **14** 2171
[17] Yang Y G, Lei H, Liu Z C, Zhou Y H and Shi W M 2016 *Quantum Inf. Process.* **15** 2487
[18] Guo Y, Feng Y, Huang D and Shi J 2016 *Int. J. Theor. Phys.* **55** 2290
[19] Shang T, Zhao X, Wang C and Liu J 2015 *Quantum Inf. Process.* **14** 393
[20] Wang B, Yang H and Meng F 2017 *Calcolo* **54** 117
[21] Su Qi, Huang Z, Wen Q and L W 2010 *Opt. Commun.* **283** 4408
[22] Wang T Y and Wen Q Y 2010 *Chin. Phys. B* **19** 060307

[23] Shi J J, Shi R H, Guo Y and Peng X Q 2013 *Sci. China-Inform. Sci.* **56** 1
[24] Fan L, Zhang H J, Qin S L and Guo F Z 2016 *Int. J. Theor. Phys.* **55** 1028
[25] Yang Y G and Wen Q Y 2008 *Sci. China Ser. G: Phys., Mech. Astron.* **51** 1505
[26] Wen X, Tian Y, Ji L and Niu X 2010 *Phys. Scr.* **81** 055001
[27] Shi J, Shi R, Tang Y and Lee M H 2011 *Quantum Inf. Process.* **10** 653
[28] Xu G B and Zhang K J 2015 *Quantum Inf. Process.* **14** 2577
[29] Wang T Y and Wei Z L 2012 *Quantum Inf. Process.* **11** 455
[30] Gottesman D and Chuang I 2001 arXiv preprint quant-ph0105032
[31] Collins R J, Donaldson R J, Dunjko V, Wallden P, Clarke P J, Andersson E, Jeffers J and Buller G S 2014 *Phys. Rev. Lett.* **112** 040502
[32] Yin H L, Fu Y and Chen Z B 2016 *Phys. Rev. A* **93** 032316
[33] Li W, Shi R, Huang D, Shi J and Guo Y 2016 *Phys. Scr.* **91** 035101
[34] Liu J L, Shi R H, Shi J J, Lv G L and Guo Y 2016 *Chin. Phys. B* **25** 080306
[35] Braunstein S L and Van Loock P 2005 *Rev. Mod. Phys.* **77** 513
[36] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[37] Scarani V, Acin A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901
[38] Takei N, Aoki T, Koike S, Yoshino K, Wakui K, Yonezawa H, Hiraoka T, Mizuno J, Takeoka M, Ban M and Furusawa A 2005 *Phys. Rev. A* **72** 042304
[39] Zeng G, Lee M, Guo Y and He G 2007 *Int. J. Quantum Inf.* **5** 553
[40] Ma H, Huang P, Bao W and Zeng G 2016 *Quantum Inf. Process.* **15** 2605
[41] Jouguet P, Kunz-Jacques S and Leverrier A 2011 *Phys. Rev. A* **84** 062317
[42] Cerf N J, Levy M and Van Assche G 2001 *Phys. Rev. A* **63** 052311
[43] Guo Y, Liao Q, Wang Y, Huang D, Huang Peng and Zeng G 2017 *Phys. Rev. A* **95** 032304
[44] Guo Y, Xie C, Liao Q, Zhao W, Zeng G and Huang D 2017 *Phys. Rev. A* **96** 022320
[45] Huang D, Huang P, Lin D and Zeng G 2016 *Sci. Rep.* **6** 19201
[46] Li Y M, Wang X Y, Bai Z L, Liu W Y, Yang S S and Peng K C 2017 *Chin. Phys. B* **26** 040303
[47] Einstein A, Podolsky B and Rosen N 1935 *Phys. Rev.* **47** 777
[48] Walls D F and Milburn G J 2007 *Quantum Optics* (Springer Science, Business Media)
[49] Jeong H, Ralph T C and Bowen W P 2007 *J. Opt. Soc. Am. B* **24** 355
[50] Furusawa A, Sfrensen J L, Braunstein S L, Fuchs C A, Kimble H J and Polzik E S 1998 *Science* **282** 706
[51] Twamley J 1996 *J. Phys. A: Math. Gen.* **29** 3723
[52] Andersson E, Curty M and Jex I 2006 *Phys. Rev. A* **74** 022304
[53] Gao F, Qin S J, Guo F Z and Wen Q Y 2011 *Phys. Rev. A* **84** 022344
[54] Kogias I, Ragy S and Adesso G 2014 *Phys. Rev. A* **89** 052324