SCIENTIFIC REP⚙RTS

Gaussian private quantum channel with squeezed coherent states

Kabgyun Jeong[1], Jaewan Kim[1] & Su-Yong Lee[2]

While the objective of conventional quantum key distribution (QKD) is to secretly generate and share the classical bits concealed in the form of maximally mixed quantum states, that of private quantum channel (PQC) is to secretly transmit individual quantum states concealed in the form of maximally mixed states using shared one-time pad and it is called Gaussian private quantum channel (GPQC) when the scheme is in the regime of continuous variables. We propose a GPQC enhanced with squeezed coherent states (GPQCwSC), which is a generalization of GPQC with coherent states only (GPQCo) [Phys. Rev. A 72, 042313 (2005)]. We show that GPQCwSC beats the GPQCo for the upper bound on accessible information. As a subsidiary example, it is shown that the squeezed states take an advantage over the coherent states against a beam splitting attack in a continuous variable QKD. It is also shown that a squeezing operation can be approximated as a superposition of two different displacement operations in the small squeezing regime.

The notion of private quantum channel (PQC) or quantum one-time pad[1] is very useful in quantum information processing, such as superdense coding[2], quantum data hiding[3], quantum state sharing protocol[4] (for improving their efficiency), and the proof of additivity counter-example of the classical capacity on quantum channels[5,6]. The PQC is briefly introduced as follows. If the two communicating parties, Alice and Bob, share a classical secret key (e.g., via quantum key distribution procedure), then PQC can be used to transmit an arbitrary unknown quantum state from Alice to Bob securely. The intermediate state in PQC is close to the maximally mixed state, so the state exhibits almost maximum entropy. The receiver Bob always decrypts the encoded state by using the unitary inverse operations from the pre-shared secret key, whereas no third party (not having the key) can obtain the original quantum state. Private quantum channel which belongs to a completely positive and trace preserving-map, represents the transformation of any quantum states into the maximally mixed state. It is different from the private capacity of quantum channels[7–9] that is the maximally transmitted rate of classical secret information on quantum channels. A discrete version of private quantum channel was first proposed by Ambainis *et al.*[1] in 2000, and the optimality of PQC was proved that we need exactly d^2 unitary operations to encrypt a d-dimensional quantum state[10,11]. In the case of approximate encryption, it is sufficient to have the number of unitary operations being less than $d \log d$[3,12,13].

Then, it is natural to ask how we can realize the PQC in continuous variable (CV) systems. Previously Brádler proposed CV private quantum channel (PQC) using coherent states that are obtained by displacement operations on the vacuum state[14], where he defined a CV maximally mixed state in Gaussian regime and then constructed GPQC via the *conformation* method of coherent states. Generally a single-mode Gaussian state is parametrized as a combination of displacement, squeezing operations and a thermal field[15]. Specifically squeezed states, which were considered in CV quantum key distribution[16–20], are crucial for a security demonstration of quantum key distribution using coherent states[21]. Moreover squeezed coherent states are useful for enhancing the security of quantum cryptography[22,23], and for improving phase sensitivities of interferometers[24].

In this paper, we generalize the Gaussian private quantum channel (GPQC) with a combination of displacement and *squeezing* operations. Explicitly, we construct GPQC in terms of the displacement and

[1]School of Computational Sciences, Korea Institute for Advanced Study, Hoegiro 85, Dongdaemun, Seoul 130-722, Korea. [2]Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117543, Singapore. Correspondence and requests for materials should be addressed to K.J. (email: kgjeong6@kias.re.kr) or J.K. (email: jaewan@kias.re.kr) or S.-Y.L. (email: papercrane79@gmail.com)

the squeezing elements, $\exp\left[-r_p^2\left\{1 - \tanh r \cdot \cos\left(2\theta_{pq} - \phi\right)\right\}\right]$ whereas Brádler's GPQC is represented only by the displacement element, $\exp\left(-r_p^2\right)$. Then, we study a subsidiary example of GPQC with squeezed coherent states (GPQCwSC), especially for an eavesdropping attack. In the limit of small squeezing, furthermore, we show that the squeezed coherent states can approach a non-Gaussian regime by replacing the squeezing operation with a non-Gaussian operation, i.e., a superposition operation of two different displacements.

Gaussian private quantum channel (GPQC): coherent states

Gaussian private quantum channel (GPQC) was introduced by Brádler in 2005, where he defined a maximally mixed state as $\mathbb{1}_b$ in Gaussian regime[14]. Similarly to the discrete case (identity over the dimension: $\mathbb{1}/d$), the CV maximally mixed state in phase space has a broad Gaussian shape (because equiprobable mixture depends only on the radius at some boundary). Brádler's main proposition is that the Hilbert-Schmidt distance d_{HS} between the CV maximally mixed state and PQC-encryption of arbitrary coherent states is very close for sufficiently large N (N: number of input displacement operations),

$$d_{HS}\left(\mathbb{1}_b, \Gamma_N\right) \approx \sqrt{N^{-2} + O(N^{-4})} \ll 1, \tag{1}$$

where Γ_N denotes the mixture of all conformations of coherent states that will be defined in Eqs (3) and (4). Also note that $d_{HS}(\rho_1, \rho_2) := \sqrt{\mathbf{tr}\left(\rho_1 - \rho_2\right)^2}$ for any matrices $\rho_{1,2}$ and it is symmetric, $d_{HS}(\rho_1, \rho_2) = d_{HS}(\rho_2, \rho_1)$. By using the unitary invariance of the distance, we can prove the statement on an arbitrary coherent state $|\beta\rangle$: for $|\beta\rangle$ and CV private quantum channel $\mathcal{N}_N$, $d_{HS}\left(\mathbb{1}_b^\beta, \mathcal{N}_N(|\beta\rangle\langle\beta|)\right) = d_{HS}\left(\mathbb{1}_b, \Gamma_N\right)$, where $\mathbb{1}_b^\beta$ is a displaced CV maximally mixed state from $\mathbb{1}_b$ to the position of $|\beta\rangle$. The proof is a bit complex but straightforward (See details in Ref.14).

Now we review the (Brádler's) CV maximally mixed state[14]. A CV maximally mixed state can be chosen as an integral performed over all possible single mode states within the boundary circle of radius $r \leq b$ in a coherent state $|\alpha\rangle$. If $r > b$, the occurrence probability is 0. The coherent state is created by applying the displacement operator $\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}$ to the vacuum state $|0\rangle$ as $|\alpha\rangle = \hat{D}(\alpha)|0\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle$. Then, we have the CV maximally mixed state

$$\begin{aligned}\mathbb{1}_b &= \frac{1}{C}\int|\alpha\rangle\langle\alpha|d^2\alpha \\ &= \frac{1}{b^2}\sum_{n=0}^{\infty}\left(1 - \sum_{k=0}^{n}\frac{b^{2k}}{k!}e^{-b^2}\right)|n\rangle\langle n|,\end{aligned} \tag{2}$$

where the normalization constant is $C = \pi b^2$.

The purpose of GPQC is to encrypt an input coherent state into a high entropy state. Thus the encryption should be close to the maximally mixed state in Hilbert-Schmidt distance. In order to do that, we introduce a notion of conformation through vacuum displacements. Note that $\alpha_{pq} = r_p e^{i\theta_{pq}}$ for $\theta_{pq} = \frac{\pi}{p}(2q - 1)$, where p and q are positive integers. For some fixed p, an input coherent state is described by $|\alpha_{pq}\rangle = |r_p e^{i\theta_{pq}}\rangle = e^{-r_p^2/2}\sum_{m=0}^{\infty}\frac{\left(r_p e^{i\theta_{pq}}\right)^m}{\sqrt{m!}}|m\rangle$. From the Ref. 14, the general and slightly modified p-conformation ($p \in \mathbb{Z}^+$) is given by the following equations

$$\begin{aligned}\rho_p &= \frac{1}{p}\sum_{q=1}^{p}|\alpha_{pq}\rangle\langle\alpha_{pq}| \\ &= \frac{e^{-r_p^2}}{p}\sum_{q=1}^{p}\sum_{m,n=0}^{\infty}\frac{r_p^{m+n}}{\sqrt{m!n!}}e^{i\theta_{pq}(m-n)}|m\rangle\langle n| \\ &= \frac{e^{-r_p^2}}{p}\sum_{m,n=0}^{\infty}\frac{r_p^{m+n}}{\sqrt{m!n!}}e^{-\frac{i\pi}{p}(m-n)}\sum_{q=1}^{p}e^{\frac{2\pi i}{p}q(m-n)}|m\rangle\langle n| \\ &= e^{-r_p^2}\sum_{m,n=0}^{\infty}\frac{r_p^{m+n}}{\sqrt{m!n!}}(-1)^{\frac{m-n}{p}}\delta_{m=n(\text{mod } p)}|m\rangle\langle n|,\end{aligned} \tag{3}$$

$$= e^{-r_p^2}\sum_{m,n=0}^{\infty}\frac{r_p^{m+n}}{\sqrt{m!n!}}|m\rangle\langle n|\delta_{m,n(\text{mod } p)}, \tag{4}$$

where $\sum_{q=1}^{p} e^{\frac{2\pi i}{p} q(m-n)} = p$ for $m = n \bmod p$, and 0 for otherwise. The Eq. (4) is followed by the absorption of the phase term into $|m\rangle$'s and $|n\rangle$'s. This is equivalent to the Brádler's original p-conformation. The conformation technique provides an equiprobable positioning of vacuum states at some fixed radius r_p, so the uniformity of the distribution of CV quantum states is strengthened.

Finally we review the mixture of all p-conformations ($p = 1, \ldots, N$). Suppose that $N \geq 1$ and define $r_p = \frac{(p-1)b}{N} \leq b$, then

$$\Gamma_N = \frac{1}{M} \sum_{p=1}^{N} p \rho_p = \frac{1}{M} \sum_{p=1}^{N} \sum_{q=1}^{p} \hat{D}(\alpha_{pq}) |0\rangle \langle 0| \hat{D}^{\dagger}(\alpha_{pq}),$$

(5)

where $M = N(N+1)/2$. As an encrypted state of GPQC, the Γ_N represents the output state of PQC over (uniformly chosen) M unitary operations, where the input state is in vacuum state $|0\rangle \langle 0|$. One of the M CV states is fixed by pre-shared classical secret key between Alice and Bob as (classical) one-time pad, and then it is sent to Bob. The Brádler's proposition states that Γ_N is sufficiently close to the CV maximally mixed state. Encoding an arbitrary coherent state $|\beta\rangle$ is essentially equivalent to the vacuum state encryption for the unitary invariance of the distance: $d_{HS} \left(\mathbb{1}_b^{\beta}, \mathcal{N}_N(|\beta\rangle\langle\beta|) \right) = d_{HS} \left(\mathbb{1}_b, \Gamma_N \right)$. Also note that, for any completely positive and trace-preserving (CPT) map $\mathcal{N}_N$, $\mathcal{N}_N(|\beta\rangle \langle \beta|) = \hat{D}(\beta) \Gamma_N \hat{D}^{\dagger}(\beta)$ (See Eq. (9) in Ref. 14). Therefore we derive Brádler's main result as Eq. (1) by combining the above properties of CV maximally mixed state, p-conformation, and its mixture.

Results

Gaussian private quantum channel: squeezed coherent states. To construct a GPQCwSC, we examine a single-mode squeezed vacuum state. A single-mode squeezing operation is defined by $\hat{S}(\xi) = \exp\left[\frac{\xi^* \hat{a}^2 - \xi \hat{a}^{\dagger 2}}{2}\right]$, where $\xi = re^{i\phi}$. When we apply the squeezing operator to the vacuum state, we produce a squeezed vacuum state such that

$$|\xi, 0\rangle := \frac{1}{\sqrt{\cosh r}} \sum_{n=0}^{\infty} \frac{\sqrt{(2n)!}}{2^n n!} \left(-e^{i\phi} \tanh r\right)^n |2n\rangle.$$

Then, applying a displacement operation, we obtain a coherent squeezed state $\left(|\alpha, \xi\rangle = \hat{D}(\alpha) \hat{S}(\xi) |0\rangle\right)$ which forms an overcomplete set, i.e., $\frac{1}{\pi} \int d^2\alpha |\alpha, \xi\rangle \langle \alpha, \xi| = \mathbb{1}$[25]. It is a main ingredient of the squeezed CV conformation.

For simplicity, we consider a squeezed coherent state, instead of the coherent squeezed state. It is reasonable that squeezed coherent states are transformed into coherent squeezed states by the relation, $\hat{S}(\xi) \hat{D}(\alpha) |0\rangle = \hat{D}(\alpha \cosh r - \alpha^* e^{i\phi} \sinh r) \hat{S}(\xi) |0\rangle$[25]. Generally, a squeezed coherent state represents squeezing of a coherent state[26],

$$
\begin{aligned}
|\xi, \alpha\rangle &= \hat{S}(\xi) \hat{D}(\alpha) |0\rangle \\
&= \frac{(\nu/2\cosh r)^{m/2}}{\sqrt{\cosh r \cdot m!}} \exp\left[-\frac{1}{2}\left(|\alpha|^2 - \frac{\nu^* \alpha^2}{\cosh r}\right)\right] \\
&\quad \times H_m\left(\frac{\alpha}{\sqrt{2\nu \cosh r}}\right) |m\rangle,
\end{aligned}
$$

(6)

where $\nu := e^{i\phi} \sinh r$ and $\phi = \arg(\xi)$, the argument of the squeezing parameter ξ. $H_m(\cdot)$ denotes the mth-degree complex Hermite polynomials. By exploiting the Eq. (6), we can derive a squeezed conformations and its mixture in the following section. Then we prove that, for sufficiently large N and for any squeezing of a coherent state $|\beta\rangle$, there exists a CPT map $\mathcal{N}$ such that $d_{HS} \left(\mathbb{1}_b^{(\beta,\xi)}, \mathcal{N}_N(\xi, |\beta\rangle\langle\beta|) \right) \ll 1$. (See following second section.)

General squeezed conformations. Now, we show the explicit calculation of the squeezed p-conformation. Let us apply the squeezing operation to the coherent state $(|\alpha_{pq}\rangle)$,

$$
\begin{aligned}
\hat{S}(\xi) |\alpha_{pq}\rangle &= \sum_{m=0}^{\infty} \frac{\left(\frac{\nu}{2\cosh r}\right)^{m/2}}{\sqrt{\cosh r \cdot m!}} e^{-\frac{1}{2}\left(|\alpha_{pq}|^2 - \frac{\nu^* \alpha_{pq}^2}{\cosh r}\right)} \\
&\quad \times H_m\left(\frac{\alpha_{pq}}{\sqrt{2\nu \cosh r}}\right) |m\rangle,
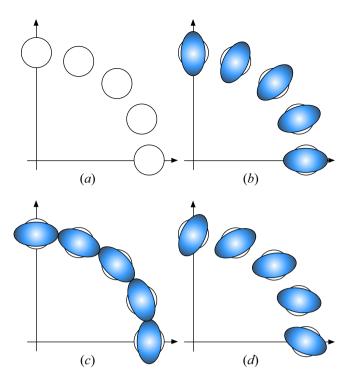\end{aligned}
$$

(7)

Figure 1. For some fixed r and r_p, the argument $(0 \leq \phi < 2\pi)$ of ξ depends on $\theta_{pq} \ \forall \ q \in \mathbb{Z}^+$. This figure represents the squeezed 16th-conformation $(r_p = r_{16})$ in the factor $K = 1 - \tanh r \cdot \cos(2\theta_{pq} - \phi)$: (a) non-squeezed $(r = 0)$, (b) $\phi = 0$, (c) $\phi = \pm\frac{\pi}{2}$, and (d) $\phi = -\frac{\pi}{4}$ cases, respectively.

where $\alpha_{pq} = r_p e^{i\theta_{pq}}$ and $\nu = e^{i\phi}\sinh r$ (p and q are positive integers). Using the following relations: $\nu^*\alpha_{pq}^2 + \nu\alpha_{pq}^{*2} = r_p^2 \sinh r \left(e^{i(2\theta_{pq} - \phi)} + e^{-i(2\theta_{pq} - \phi)}\right) = 2r_p^2 \sinh r \cos(2\theta_{pq} - \phi)$ and $2 \sinh r \cdot \cosh r = \sinh(2r)$, then we derive the formula

$$\hat{S}(\xi)|\alpha_{pq}\rangle\langle\alpha_{pq}|\hat{S}^\dagger(\xi) = \sum_{m,n} \frac{\left(\frac{\tanh r}{2}\right)^{(m+n)/2}}{\cosh r\sqrt{m!n!}} e^{i\phi(m-n)/2} \cdot e^{-Kr_p^2}$$
$$\times H_m\left(\frac{r_p e^{i\left(\theta_{pq} - \frac{\phi}{2}\right)}}{\sqrt{\sinh(2r)}}\right) H_n(c.c.)|m\rangle\langle n|,$$

$$(8)$$

where $K := 1 - \tanh r \cdot \cos(2\theta_{pq} - \phi)$ and *c.c.* denotes the complex conjugate of the argument of H_m. The definition of K determines the position of squeezed coherent states and the squeezing angles, as shown in Fig. 1.

Then, we can find the squeezed p-conformation

$$\rho_p^\xi = \frac{1}{P}\sum_{q=1}^P \hat{S}(\xi)|\alpha_{pq}\rangle\langle\alpha_{pq}|\hat{S}^\dagger(\xi)$$
$$= \sum_{m,n=0}^\infty \kappa_{m,n} \cdot e^{-r_p^2\left\{1 - \tanh r \cdot \cos(2\theta_{pq} - \phi)\right\}}|m\rangle\langle n|,$$

$$(9)$$

where $\theta_{pq} = \frac{\pi}{p}(2q - 1)$ and the constant $\kappa_{m,n}$ is defined by

$$\kappa_{m,n} := \frac{1}{P}\sum_{q=1}^P \frac{(\tanh r/2)^{(m+n)/2}}{\cosh r\sqrt{m!n!}} \exp\left[i\frac{\phi}{2}(m - n)\right]$$
$$\times H_m\left(\frac{r_p e^{i\left(\theta_{pq} - \frac{\phi}{2}\right)}}{\sqrt{\sinh(2r)}}\right) H_n(c.c.).$$

$$(10)$$

For some fixed squeezing r and the argument ϕ, the (complex) Hermite polynomials are orthogonal to each other for $m \neq n$ such that the value of $\kappa_{m,n}$ becomes a constant. The $\kappa_{m,n}$ converges to $r_p^{m+n}/\sqrt{m!n!}$ as $r \to 0$. Therefore, the factor for some p, $\exp\left[-r_p^2\left\{1 - \tanh r \cdot \cos\left(2\theta_{pq} - \phi\right)\right\}\right]$, is the main component in Eq. (9).

We finally consider the mixture of all squeezed p-conformations for $0 \leq p \leq N$. Suppose $N \geq 1$ and define $r_p = \frac{(p-1)b}{N} \leq b$, then

$$\Gamma_N^\xi = \frac{1}{M}\sum_{p=1}^{N}\sum_{q=1}^{p}\hat{S}(\xi)\hat{D}(\alpha_{pq})|0\rangle\langle 0|\hat{D}^\dagger(\alpha_{pq})\hat{S}^\dagger(\xi),$$
(11)

where $M = N(N+1)/2$. Alice equiprobably chooses one from the set of M displacement operators $\hat{D}(\alpha_{pq}) = e^{\alpha_{pq}\hat{a}^\dagger - \alpha_{pq}^*\hat{a}}$ and the squeezing parameter $r > 0$. (Once again note that, for some fixed p and r, the squeezing argument ϕ depends on θ_{pq} for all q.) Alice sends the encrypted state through a quantum channel towards Bob who performs the inverse operations to decrypt the state.

The point is that we encrypt an arbitrary input state, i.e., an arbitrary coherent state ($|\beta\rangle$). Then, we can write down a general encryption CPT map $\mathcal{N}$ with M unitary elements as in Ref. 14

$$\begin{aligned}
\mathcal{N}_N(\xi, |\beta\rangle\langle\beta|) &= \frac{1}{M}\sum_{p=1}^{N}\sum_{q=1}^{p}\hat{S}(\xi)\hat{D}(\alpha_{pq})\hat{D}(\beta)|0\rangle\langle 0|\hat{D}^\dagger(\beta)\hat{D}^\dagger(\alpha_{pq})\hat{S}^\dagger(\xi) \\
&= \frac{1}{M}\sum_{p=1}^{N}\sum_{q=1}^{p}\hat{S}(\xi)\hat{D}(\beta)\hat{D}(\alpha_{pq})|0\rangle\langle 0|\hat{D}^\dagger(\alpha_{pq})\hat{D}^\dagger(\beta)\hat{S}^\dagger(\xi) \\
&= \hat{S}(\xi)\hat{D}(\beta)\Gamma_N\hat{D}^\dagger(\beta)\hat{S}^\dagger(\xi).
\end{aligned}$$

From the above equation, we propose that the corresponding Hilbert-Schmidt (HS) distance is equivalent to one of Eq. (11), $d_{HS}\left(\mathbb{1}_b^{(\beta,\xi)}, \mathcal{N}_N(\xi, |\beta\rangle\langle\beta|)\right) = d_{HS}(\mathbb{1}_b, \Gamma_N^\xi)$ by the unitary invariance of the HS distance, whereas the states are not the same as $\mathcal{N}_N(\xi, |\beta\rangle\langle\beta|) \neq \Gamma_N^\xi$.

The proof of the main proposition and the number of secret bits. Here we prove our main proposition. The proposition is as follow: For sufficiently large N in any squeezing of an arbitrary coherent state $|\beta\rangle$, there exists CPT map $\mathcal{N}_N$ such that

$$d_{HS}\left(\mathbb{1}_b^{(\beta,\xi)}, \mathcal{N}_N(\xi, |\beta\rangle\langle\beta|)\right) \leq d_{HS}\left(\mathbb{1}_b, \Gamma_N\right)$$
(12)

$$\approx \sqrt{N^{-2} + O\left(N^{-4}\right)},$$
(13)

where the HS distance between $\mathbb{1}_b$ and Γ_N^ξ becomes quite close in sufficiently large N. The Eq. (12) is obtained from the unitary invariance of the HS distance. The Eq. (13) is derived via the unitary invariance of squeezing operations in the HS distance (Eq. (14) below) and it is followed by the norm convexity (Eq. (15)). Explicitly speaking, in the case of $\xi > 0$, we assert that ($N \gg 1$)

$$\begin{aligned}
d_{HS}(\Gamma_N^\xi, \Gamma_N) &= d_{HS}\left(\hat{S}(\xi)\Gamma_N\hat{S}^\dagger(\xi), \Gamma_N\right) \\
&= d_{HS}\left(\hat{S}(\xi)|0\rangle\langle 0|\hat{S}^\dagger(\xi), |0\rangle\langle 0|\right) \simeq 0,
\end{aligned}$$
(14)

where the second equality also holds by the unitary invariance in the HS distance, i.e., for all unitary $\hat{U} := \hat{S}\hat{D}$ and $\hat{U}' := \hat{D}\hat{S}$, $d_{HS}(\hat{U}|0\rangle\langle 0|\hat{U}^\dagger, \hat{D}|0\rangle\langle 0|\hat{D}^\dagger) = d_{HS}(\hat{U}'|0\rangle\langle 0|\hat{U}'^\dagger, \hat{D}|0\rangle\langle 0|\hat{D}^\dagger) = d_{HS}(\hat{S}|0\rangle\langle 0|\hat{S}^\dagger, |0\rangle\langle 0|)$. In general, the last equality is not exactly equal to zero, but, asymptotically converges to 0, i.e., $d_{HS}(\hat{S}|0\rangle\langle 0|\hat{S}^\dagger, |0\rangle\langle 0|) = \frac{2\sinh(r/2)}{\sqrt{\cosh r}} \simeq 0$[27].

Therefore, by using the norm convexity and the above equations (within the symmetric property of the HS distance) we derive

$$d_{HS}(\mathbb{1}_b, \Gamma_N^\xi) \leq d_{HS}(\mathbb{1}_b, \Gamma_N) + d_{HS}(\Gamma_N^\xi, \Gamma_N)$$
(15)

$$\simeq d_{HS}(\mathbb{1}_b, \Gamma_N) \approx (N+1)^{-1}.$$

Thus, it implies that $\mathbb{1}_b$ approximately equals to the sum of the squeezed coherent states, and therefore completes the proof.

In addition, we mention the total number of unitary operations L and corresponding secret bits. The number of total displacement is $M = N(N+1)/2$ and just one (pre-fixed) squeezing operation is required. From this reason, $L = M + 1$. Thus, we have the number of secret bits of $\ell = \log L \sim 2\log N$ for $N \gg 1$. It is interesting to note that if we use the approximate random unitary channels such as in Refs. 3,12,13, then it is expected to construct PQC with only about $\frac{\ell}{2}$-bits of secret keys. There is no advantage in the key efficiency, but the accessible information can be slightly improved as follow.

Holevo bound on the GPQCwSC.   One of important principles of the von Neumann entropy states that quantum operations never increase the quantum mutual information. By using this property, we propose that our GPQCwSC is stronger (i.e., tight upper bound) than the Brádler's GPQC in the language of accessible information.

Formally, Brádler's protocol[14] with coherent states consists of a set of $\{\mathcal{C}, p_{\mathcal{C}}, \mathcal{N}_N(|\beta\rangle\langle\beta|), \mathbb{1}_b^\beta\}$, where $\mathcal{C}$ denotes the set of all coherent states $|\beta\rangle$, $p_{\mathcal{C}}$ is the probability distribution of $\mathcal{C}$, $\mathcal{N}_N(\cdot)$ is the CPT map with N displacement operations, and $\mathbb{1}_b^\beta$ is the (displaced) CV maximally mixed state. Similarly, let us express our GPQCwSC as a set of $\{\mathcal{S}, p_{\mathcal{S}}, \mathcal{N}_N(\xi, |\beta\rangle\langle\beta|), \mathbb{1}_b^{(\beta,\xi)}\}$, where squeezing elements are added and the set $\mathcal{S}$ emphasizes the squeezing with displacement operations. Then we assert that $(\beta := |\beta\rangle\langle\beta|)$

$$\chi\big(\{\mathcal{S}, p_{\mathcal{S}}, \mathcal{N}_N(\xi, \beta), \mathbb{1}_b^{(\beta,\xi)}\}\big) \leq \chi\big(\{\mathcal{C}, p_{\mathcal{C}}, \mathcal{N}_N(\beta), \mathbb{1}_b^\beta\}\big), \tag{16}$$

where the Holevo information $\chi := \max_{\mathcal{E}} I_{acc}(B:E)$. The B and E are corresponding to input and output distributions of the channel $\mathcal{N}_N(\cdot)$ between Bob and Eve, and the maximum of the accessible information (by Eve) is taken over all input ensemble $\mathcal{E}$ in the channel. Note that the quantum mutual information is defined by $I(A:B) = S(A) + S(B) - S(AB)$ for any quantum system A and B, where $S(\sigma) = -\mathbf{tr}\sigma \log \sigma$ is the von Neumann entropy. This fact directly comes from 'the principle of quantum operation' about the entropy: For any quantum operation Q, $I_{acc}(Q(B):Q(E)) \leq I_{acc}(B:E)$. If we substitute Q to a squeezing operation $\hat{S}$, and define $B := \hat{D}(\mathcal{E}_1)$ and $E := \hat{D}(\mathcal{E}_2)$ for some ensembles $\mathcal{E}_1$ and $\mathcal{E}_2$, respectively, then we have

$$I_{acc}(\hat{S}(\hat{D}(\mathcal{E}_1) : \hat{D}(\mathcal{E}_2))) \leq I_{acc}(\hat{D}(\mathcal{E}_1): \hat{D}(\mathcal{E}_2)). \tag{17}$$

This provides a better upper bound on the accessible information χ than the Brádler's analysis. In other words, the amount of eavesdropping information on the encrypted state via the GPQCwSC is less than that by the Brádler's GPQC.

Subsidiary example of GPQC.   We introduce a simple example that squeezed coherent states can take an advantage over coherent states in CV quantum key distribution, where the scheme is in a preliminary procedure of GPQC. To distribute quantum keys, we consider the BB84 protocol[28]. In discrete variable systems, Alice and Bob share keys with single photon states in mutually unbiased bases. In continuous variable (CV) systems, correspondingly, Alice and Bob share keys with Gaussian states in uncertainty relation of field quadratures. Then, in the limit of small squeezing, we show that the squeezed coherent state scheme can approach even a non-Gaussian regime by replacing a squeezing operation with a superposition operation of two different displacements.

Simple eavesdropping attack in CV quantum key distribution.   As a simple eavesdropping attack, we assume that Eve performs a beam splitting attack. As an input state, we compare a squeezed coherent state with a coherent one. For an input squeezed coherent state, Eve transforms the input state by a 50:50 beam splitter,

$$\hat{B}_{BE}\hat{S}_B(\xi)\hat{D}_B(\alpha)|0\rangle_B|0\rangle_E = \hat{S}_B\left(\frac{\xi}{2}\right)\hat{S}_E\left(\frac{\xi}{2}\right)\hat{S}_{BE}\left(\frac{\xi}{2}\right)\hat{D}_B\left(\frac{\alpha}{2}\right)\hat{D}_E\left(\frac{\alpha}{2}\right)|0\rangle_B|0\rangle_E, \tag{18}$$

where the subscript B (E) represents Bob (Eve), and the transformation of the squeezing operation is given by Ref. 29. When Eve performs a measurement to get an information of the input state $(|\cdot\rangle_E)$, the state $(|\cdot\rangle_B)$ sent to Bob is disturbed by the non-local effect of the two-mode squeezing operation $\hat{S}_{BE}\left(\frac{\xi}{2}\right)$, except the uncertainty of the field quadrature. For an input coherent state, there is no non-local effect after the beam splitting attack. For the beam splitting attack, thus, Alice and Bob detect the existence of Eve much easier with the input squeezed coherent state than the input coherent one.

Figure 2. Optical implementation for a superposition operation of two different displacements. The beam splitter is highly reflective.

Non-Gaussian regime. We show that the squeezed coherent state can approach even a non-Gaussian regime. In the limit of small squeezing, we describe a non-Gaussian regime by a truncation of the squeezing parameter, $\hat{S}(\xi) \approx 1 - \frac{\xi}{2}\hat{a}^{\dagger 2} + \frac{\xi^*}{2}\hat{a}^2$. However the truncation operation is not implemented by reducing the squeezing parameter in experiment. In order to apply the truncation operation to coherent states, we consider a superposition operation of two different displacements. Since an even coherent state is quite similar to a squeezed vacuum state, we derive the corresponding parameters in the limit of r, $|\beta|^2 \ll 1$,

$$\left| \frac{\langle \beta | + \langle -\beta |}{\sqrt{2(1 + e^{-2|\beta|^2})}} |\xi, 0\rangle \right|^2 \approx 1 - |\beta|^2 r \, \cos(2\phi - \varphi), \tag{19}$$

where $\beta = |\beta|e^{i\varphi}$ and $\xi = re^{i\phi}$. When $\varphi = 2\phi \pm \pi/2$, the even coherent state is approximated to the squeezed vacuum state. Note that, for $|\beta|^2 \ll 1$, the even coherent state is close to a Gaussian state but it is a non-Gaussian state[30]. Therefore, the variables r and ϕ in the squeezing parameter can be replaced by the ones β and φ in the even coherent state.

We need to know if the uncertainties of the field quadratures are maintained by replacing the squeezed vacuum state with the even coherent state. Because CV quantum key distribution is secured via uncertainties of field quadratures[16–18]. Using the quadrature operator $\hat{X}_\theta = (\hat{a}e^{-i\theta} + \hat{a}^\dagger e^{i\theta})/2$, we derive the quadrature variance of the squeezed vacuum state as

$$\begin{aligned} \Delta X_\theta^2 \big|_{sv} &= \frac{1}{4}[\cosh(2r) - \sinh(2r)\cos(2\theta - \phi)] \\ &\approx \frac{1}{4}[1 - 2r \, \cos(2\theta - \phi)], \end{aligned} \tag{20}$$

where the quadrature variance is approximated for $r \ll 1$. According to the phase parameter ϕ, the quadrature variance oscillates between $(1 - 2r)/4$ and $(1 + 2r)/4$. The quadrature variance of the even coherent state is given by

$$\begin{aligned} \Delta X_\theta^2 \big|_{ec} &= \frac{1}{4}\left[1 + \beta^2 e^{-2i\theta} + \beta^{*2} e^{2i\theta} + \frac{2|\beta|^2(1 - e^{-2|\beta|^2})}{1 + e^{-2|\beta|^2}}\right] \\ &\approx \frac{1}{4}[1 + 2|\beta|^2 \, \cos(2\theta - 2\varphi)], \end{aligned} \tag{21}$$

where the quadrature variance is approximated for $|\beta|^2 \ll 1$. According to the phase parameter φ, the quadrature variance oscillates between $(1 - 2|\beta|^2)/4$ and $(1 + 2|\beta|^2)/4$. For the quadrature variances, thus, $|\beta|^2$ corresponds to r. Therefore, we find that the uncertainties of the field quadratures are maintained in the substitution of the even coherent state for the squeezed vacuum state. Note that, for the beam splitting attack, the even coherent state also plays a role of a squeezing operator by generating an entangled state with a beam splitter.

Now we see how to realize the non-Gaussian operation with an optical implementation of a superposition operation of two different displacements, as shown in Fig. 2. Previously the displacement operation was implemented by a beam splitter with high reflectivity[31], where the displacement amplitude is described with the multiplication $(\gamma\sqrt{T})$ of an amplitude of coherent lights (γ) and the transmission coefficient of the beam splitter (T). In Fig. 2, the superposition operation of two different displacements is implemented by a beam splitter with high reflectivity ($T \to 0$), where $\sqrt{T}\gamma$ represents β in the superposition operation of two different displacements. Note that the input even coherent state can be generated by a nonlinear Kerr medium[32–34] in all-optical systems.

Discussion

We have constructed GPQCwSC by an equiprobable combination of squeezed coherent states in a continuous-variable regime generalizing GPQCo and shown that GPQCwSC tightens the upper bound on accessible information. We have also presented a simple intuitive understanding of the well-known fact that the squeezed state scheme has better security than the coherent state scheme in continuous variable QKD. A class of non-Gaussian operations, superpositions of two different displacements, is shown to be an approximation of small squeezing operations. With these results, we pursue an all-optical implementation of PQC feasible with available optical technology. As some non-Gaussian states are more robust against decoherence than Gaussian states[35–37], we look forward to investigating non-Gaussian quantum communications compared to GPQC with decoherence.

References

1. Ambainis, A., Mosca, M., Tapp, A. & de Wolf, R. Private quantum channels. *IEEE 54th Annual Symposium on Foundations of Computer Science* p. 547 (2000), Redondo Beach, California. (2000, November 12–14).
2. Harrow, A., Hayden, P. & Leung, D. Superdense Coding of Quantum States. *Phys. Rev. Lett.* **92,** 187901 (2004).
3. Hayden, P., Leung, D., Shor, P. W. & Winter, A. Randomizing Quantum States: Constructions and Applications. *Commun. Math. Phys.* **250,** 371 (2004).
4. Chi, D. P. & Jeong, K. Approximate Quantum State Sharings via Pair of Private Quantum Channels. *J. Quant. Info. Sci.* **4,** 64 (2014).
5. Hayden, P. & Winter, A. Counterexamples to the Maximal p-Norm Multiplicativity Conjecture for all $p > 1$. *Commun. Math. Phys.* **284,** 263 (2008).
6. Hastings, M. B. Superadditivity of communication capacity using entangled inputs. *Nature Phys.* **5,** 255 (2009).
7. Pirandola, S., García-Patrón, R., Braunstein, S. L. & Lloyd, S. Direct and Reverse Secret-Key Capacities of a Quantum Channel. *Phys. Rev. Lett.* **102,** 050503 (2009).
8. Takeoka, M., Guha, S. & Wilde, M. M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature Commun.* **5,** 5235 (2014).
9. Li, K., Winter, A., Zou, X. & Guo, G. Private Capacity of Quantum Channels is Not Additive. *Phys. Rev. Lett.* **103,** 120501 (2009).
10. Nagaj, D. & Kerenidis, I. On the optimality of quantum encryption schemes. *J. Math. Phys.* **47,** 092102 (2006).
11. Bouda, J. & Ziman, M. Optimality of private quantum channels. *J. Phys. A: Math. Theor.* **40,** 5415 (2007).
12. Dickinson, P. A. & Nayak, A. Approximate Randomization of Quantum States With Fewer Bits of Key. Quantum Computing Back Action, IIT Kanpur, *AIP Conf. Proc.* **864,** 18 (2006), Springer, New York. (2006, March 6–12).
13. Aubrun, G. On Almost Randomizing Channels with a Short Kraus Decomposition. *Commun. Math. Phys.* **288,** 1103 (2009).
14. Brádler, K. Continuous-variable private quantum channel. *Phys. Rev. A* **72,** 042313 (2005).
15. Marian, P., Marian, T. A. & Scutaru, H. Quantifying Nonclassicality of One-Mode Gaussian States of the Radiation Field. *Phys. Rev. Lett.* **88,** 153601 (2002).
16. Ralph, T. C. Continuous variable quantum cryptography. *Phys. Rev. A* **61,** 010303(R) (2000).
17. Ralph, T. C. Security of continuous-variable quantum cryptography. *Phys. Rev. A* **62,** 062306 (2000).
18. Hillery, M. Quantum cryptography with squeezed states. *Phys. Rev. A* **61,** 022309 (2000).
19. Gottesman, D. & Preskill, J. Secure quantum key distribution using squeezed states. *Phys. Rev. A* **63,** 022309 (2001).
20. Cerf, N. J., Lévy, M. & Van Assche, G. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A* **63,** 052311 (2001).
21. Grosshans, F. *et al.* Quantum key distribution using gaussian-modulated coherent states. *Nature* **421,** 238 (2003).
22. Lu, Y. J., Zhu, L. & Ou, Z. Y. Security improvement by using a modified coherent state for quantum cryptography. *Phys. Rev. A* **71,** 032315 (2005).
23. Yin, Z.-Q., Han, Z.-F., Sun, F.-W. & Guo, G.-C. Decoy state quantum key distribution with modified coherent state. *Phys. Rev. A* **76,** 014304 (2007).
24. Caves, C. M. Quantum-mechanical noise in an interferometer. *Phys. Rev. D* **23,** 1693 (1980).
25. Barnett, S. M. & Radmore, P. M. *Methods in Theoretical Quantum Optics*. Oxford University Press (1997).
26. Vogel, W. & Welsch, D.-G. *Quantum Optics*. WILEY-VCH Verlag GmbH & Co. KGaA (2006).
27. Dodonov, V. V., Man'ko, O. V., Man'ko, V. I. & Wünsche, A. Energy-sensitive and "lassical-like" Distances between Quantum States. *Phys. Scr.* **59,** 81 (1999).
28. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175–179, 8 (1984), Bangalore, India. IEEE Computer Society Press, New York. (1984, December 10-12).
29. Kim, M. S., Son, W., Bužek, V. & Knight, P. L. Entanglement by a beam splitter: Nonclassicality as a prerequisite for entanglement. *Phys. Rev. A* **65,** 032323 (2002).
30. Genoni, M. G. & Paris, M. G. A. Quantifying non-Gaussianity for quantum information. *Phys. Rev. A* **82,** 052341 (2010).
31. Lvovsky, A. I. & Babichev, S. A. Synthesis and tomographic characterization of the displaced Fock state of light. *Phys. Rev. A* **66,** 011801(R) (2002).
32. Mecozzi, A. & Tombesi, P. Distinguishable quantum states generated via nonlinear birefringence. *Phys. Rev. Lett.* **58,** 1055 (1987).
33. Yurke, B. & Stoler, D. Quantum behavior of a four-wave mixer operated in a nonlinear regime. *Phys. Rev. A* **35,** 4846 (1987).
34. Gerry, C. C. Generation of optical macroscopic quantum superposition states via state reduction with a Mach-Zehnder interferometer containing a Kerr medium. *Phys. Rev. A* **59,** 4095 (1999).
35. Sabapathy, K. K., Ivan, J. S. & Simon, R. Robustness of Non-Gaussian Entanglement against Noisy Amplifier and Attenuator Environments. *Phys. Rev. Lett.* **107,** 130501 (2011).
36. Lee, J., Kim, M. S. & Nha, H. Comment on "Role of Initial Entanglement and Non-Gaussianity in the Decoherence of Photon-Number Entangled States Evolving in a Noisy Channel". *Phys. Rev. Lett.* **107,** 238901 (2011).
37. Nha, H., Lee, S.-Y., Ji, S.-W. & Kim, M. S. Efficient Entanglement Criteria beyond Gaussian Limits Using Gaussian Measurements. *Phys. Rev. Lett.* **108,** 030503 (2012).

Acknowledgements

Author Contributions

K.J. identified and proposed the study. All the authors carried out the calculations and the analysis of results.

Additional Information

How to cite this article: Jeong, K. *et al.* Gaussian private quantum channel with squeezed coherent states. *Sci. Rep.* **5**, 13974; doi: 10.1038/srep13974 (2015).