Gaussian private quantum channel with squeezed coherent states

K. JEONG, J. KIM, and S.-Y. LEE

School of Computational Sciences,
Korea Institute for Advanced Study (KIAS), Korea

Asia-Pacific Conference & Workshop in Quantum Info. Science 2014,
National Cheng Kung University, Taiwan
14 Dec. 2014

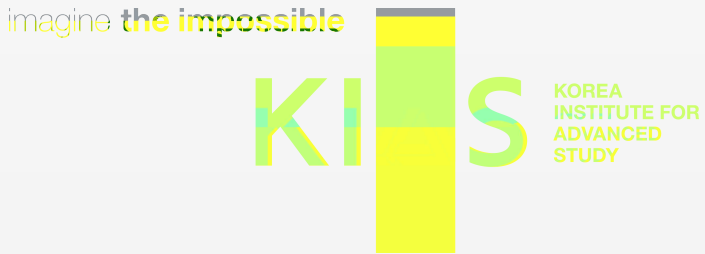


Table of contents

Preliminaries

→ Private Quantum Channel (PQC)

- Private quantum channel; quantum one-time pad; random unitary channel; ε-randomizing map; unital (qudit) channel

- For any quantum state $\rho \in \mathcal{B}(\mathbb{C}^d)$, suppose that a completely positive and trace-preserving (CPT) map $\mathcal{N} : \mathcal{B}(\mathbb{C}^d) \to \mathcal{B}(\mathbb{C}^d)$ satisfies

$$\left\| \mathcal{N}(\rho) - \frac{\mathbb{1}}{d} \right\|_p \leq \frac{\varepsilon}{\sqrt[p]{d^{p-1}}}. \tag{1}$$

  Then we say that the map $\mathcal{N}$ is ε-randomizing (or PQC) with respect to the Schatten p-norm, where $\|A\|_p = \left(\mathrm{tr}(A^\dagger A)^{p/2}\right)^{1/p}$.

- The map $\mathcal{N}$ for any ρ can be naturally constructed as follow:

$$\mathcal{N}(\rho) = \frac{1}{m} \sum_{i=1}^{m} U_i \rho U_i^\dagger,$$

  where $U_i \in \mathcal{U}(d)$ are chosen at random, and m depends on the dimension d. (e.g. $m = d^2$: optimal)

- Generally, Gaussian quantum states are represented in phase space.
- Coherent state: It 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

$$|\alpha\rangle = \hat{D}(\alpha)|0\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle.$$

  - Note that the complex number $\alpha = re^{i\theta}$; $\alpha_{pq} = r_p e^{i\theta_{pq}}$ for $\theta_{pq} = \frac{\pi}{p}(2q-1) \;\; \forall p, q \in \mathbb{Z}^+$.

- Squeezed state via squeezing operation $\hat{S}(\xi) = \exp\left[\frac{\xi^* \hat{a}^2 - \xi \hat{a}^{\dagger 2}}{2}\right]$ with $\xi = re^{i\phi}$
  - e.g., squeezed vacuum and squeezed coherent state; $\nu = e^{i\phi} \sinh r$ and $\phi = \arg(\xi)$

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

$$|\xi, \alpha\rangle = \hat{S}(\xi)\hat{D}(\alpha)|0\rangle = \frac{(\nu/2\cosh r)^{m/2}}{\sqrt{\cosh r \cdot m!}} e^{-\frac{1}{2}\left(|\alpha|^2 - \frac{\nu^* \alpha^2}{\cosh r}\right)} H_m\left(\frac{\alpha}{\sqrt{2\nu \cosh r}}\right) |m\rangle$$

- CV maximally mixed state: A CV MMS can be chosen as an integral preformed over all possible single mode states within the boundary circle of radius $r \leq b$ in a coherent state $|\alpha\rangle$ (up to a normalization constant $C = \pi b^2$).

$$\mathbb{1}_b = \frac{1}{C}\int |\alpha\rangle\langle\alpha| d^2\alpha$$
$$= \frac{1}{b^2}\sum_{n=0}^{\infty}\left(1 - \sum_{k=0}^{n}\frac{b^{2k}}{k!}e^{-b^2}\right)|n\rangle\langle n|. \quad (2)$$

- p-conformation of coherent states:
  $|\alpha_{pq}\rangle = |r_p e^{i\theta_{pq}}\rangle = e^{-r_p^2/2}\sum_{m=0}^{\infty}\frac{(r_p e^{i\theta_{pq}})^m}{\sqrt{m!}}$ ($p \in \mathbb{Z}^+$ fixed)

$$\rho_p := \frac{1}{p}\sum_{q=1}^{p}|\alpha_{pq}\rangle\langle\alpha_{pq}|$$
$$= e^{-r_p^2}\sum_{m,n=0}^{\infty}\frac{r_p^{m+n}}{\sqrt{m!n!}}|m\rangle\langle n|\delta_{m,n(\mod p)}, \quad (3)$$

where $\sum_{q=1}^{p} e^{\frac{2\pi i}{p}q(m-n)} = p$ if $m = n \mod p$.

- Mixture of all (displaced) p-conformation: For all $p = (1, \ldots, N)$ supposed that $r_p = \frac{(p-1)b}{N} \leq b$, then

$$\Gamma_N = \frac{1}{M} \sum_{p=1}^{N} p\rho_p = \frac{1}{M} \sum_{p=1}^{N} \sum_{q=1}^{p} \hat{D}(\alpha_{pq}) |0\rangle\langle 0| \hat{D}^{\dagger}(\alpha), \tag{4}$$

  where the total number of unitary operations $M = N(N+1)/2$.

- One of CV states of Γ_N is chosen at pre-shared random secret key.

- Hilbert-Schmidt distance: $d_{HS}(\rho_1, \rho_2) := \sqrt{\mathrm{tr}(\rho_1 - \rho_2)^2}$

Brádler's main result

Theorem 1: Brádler's theorem PRA 72, 042313 (2005)

For sufficiently large N, the Hilbert-Schmidt distance between the CV maximally mixed state $\mathbb{1}_b$ and PQC-encryption of arbitrary coherent states $|\beta\rangle$ is very close, i.e.,

$$d_{HS}(\mathbb{1}_b, \Gamma_N) \approx \sqrt{N^{-2} + O(N^{-4})}, \tag{5}$$

where Γ_N denotes the mixture of all conformations of coherent states.

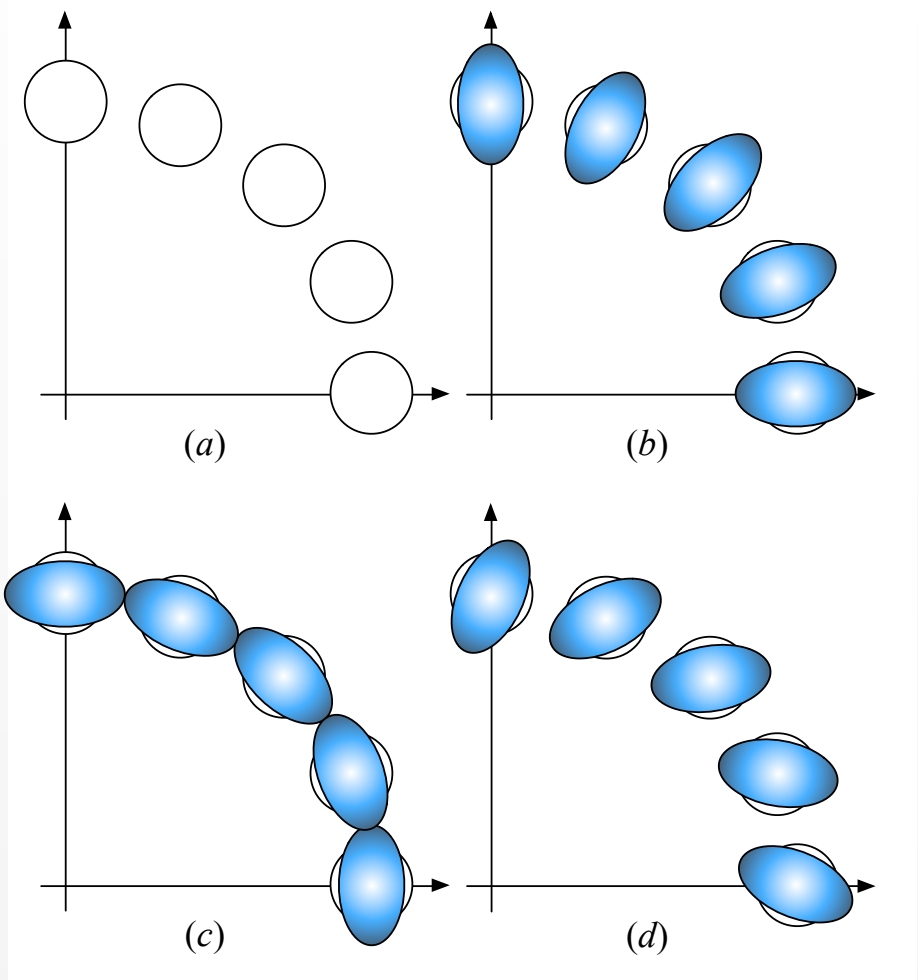
- $\mathcal{N}_N(|\beta\rangle) \neq \Gamma_N$ and $\int \hat{D}(\alpha)|\beta\rangle\langle\beta|\hat{D}^\dagger(\alpha)d^2\alpha \simeq \hat{D}(\beta)\mathbb{1}_b\hat{D}^\dagger(\beta) = \mathbb{1}_b^\beta \neq \mathbb{1}_b$, but (by unitary invariance) $d_{HS}\left[\mathbb{1}_b^\beta, \mathcal{N}_N(|\beta\rangle)\right] = d_{HS}(\mathbb{1}_b, \Gamma_N)$.
- By definition of Hilbert-Schmidt distance,

$$d_{HS}^2(\mathbb{1}_b, \Gamma_N) = \mathrm{tr}\left[(\mathbb{1}_b - \Gamma_N)^2\right] = \mathrm{tr}\left(\mathbb{1}_b\right)^2 - 2\mathrm{tr}(\mathbb{1}_b\Gamma_N) + \mathrm{tr}\left(\Gamma_N^2\right) \tag{6}$$

$$= \frac{e^{2b^2} - I_0(2b^2) - I_1(2b^2)}{b^2 e^{2b^2}} - \frac{4e^{-b^2}}{b^2 N(N+1)} \sum_{p=1}^{N} \frac{p}{e^{r_p^2}} \sum_{k=1}^{\infty} \left(\frac{b}{r_p}\right)^k I_k(2r_p b)$$

$$+ \left(\frac{2}{N(N+1)}\right)^2 \left[\sum_{p=1}^{N} \frac{p^2}{e^{2r_p^2}} \left(I_0(2r_p^2) + 2\sum_{k=1}^{\infty} I_{pk}(2r_p^2)\right) + \sum_{p_1 \neq p_2} (term)\right]$$

CVPQC vs sGPQC



For some fixed r and r_p, the **squeezed p-conformation**

- (a) non-squeezed 16-th conformation ($r = 0$)
- (b) squeezed 16-th conformation with $\phi = 0$
- (c) $\phi = \pm\frac{\pi}{2}$
- (d) $\phi = -\frac{\pi}{4}$

in K factor,

$$K = 1 - \tanh r \cdot \cos(2\theta_{pq} - \phi).$$

- CV maximally mixed state:

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

- Squeezed p-conformation of coherent states:

$$\hat{S}(\xi)|\alpha_{pq}\rangle = \sum_{m=0}^{\infty}\frac{(\nu/2\cosh r)^{m/2}}{\sqrt{\cosh r \cdot m!}}\exp\left[-\frac{1}{2}\left(|\alpha_{pq}|^2 - \frac{\nu^*\alpha_{pq}^2}{\cosh r}\right)\right] H\left(\frac{\alpha_{pq}}{\sqrt{2\nu\cosh r}}\right)|m\rangle$$

$$\rho_p^{\xi} := \frac{1}{p}\sum_{q=1}^{p}\hat{S}(\xi)|\alpha_{pq}\rangle\langle\alpha_{pq}|\hat{S}^{\dagger}(\xi)$$

$$= \sum_{m,n=0}^{\infty}\kappa_{m,n}\exp\left[-r_p^2\{1 - \tanh r\cdot\cos(2\theta_{pq} - \phi)\}\right]|m\rangle\langle n|, \qquad (7)$$

where $\theta_{pq} = \frac{\pi}{p}(2q-1)$ and the constant

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

- Mixture of squeezed p-conformations: Suppose that $N \geq 1$ and define $r_p = \frac{(p-1)b}{N} \leq b$, then

$$\Gamma_N^{\xi} = \frac{1}{M} \sum_{p=1}^{N} \sum_{q=1}^{p} \hat{S}(\xi) \hat{D}(\alpha_{pq}) |0\rangle\langle 0| \hat{D}^{\dagger}(\alpha_{pq}) \hat{S}^{\dagger}(\xi), \tag{8}$$

  where $M = N(N+1)/2$.

- Encryption of arbitrary input coherent state (via CPT map $\mathcal{N}$):

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

Squeezed Gaussian private quantum channel

KIAS

Proposition 2: Our squeezed GPQC submitted

For sufficiently large N and any squeezing of an arbitrary coherent state $|\beta\rangle$, there exists CPT map $\mathcal{N}_N$ such that

$$d_{HS}\left(\mathbb{1}_b^{(\beta,\xi)}, \mathcal{N}_N(\xi, |\beta\rangle\langle\beta|)\right) \leq d_{HS}\left(\mathbb{1}_b, \Gamma_N\right) \approx \sqrt{N^{-2} + O(N^{-4})}. \tag{9}$$

Proof :

- Unitary invariance of trace function, $d_{HS}\left(\mathbb{1}_b^{(\beta,\xi)}, \mathcal{N}_N(\xi, |\beta\rangle\langle\beta|)\right) = d_{HS}\left(\mathbb{1}_b, \Gamma_N^{\xi}\right)$
- Unitary invariance of squeezing operations,

$$\begin{aligned} d_{HS}\left(\Gamma_N^{\xi}, \Gamma_N\right) &= d_{HS}\left(\hat{S}(\xi)\Gamma_N\hat{S}^{\dagger}(\xi), \Gamma_N\right) \\ &= d_{HS}\left(\hat{S}(\xi)|0\rangle\langle 0|\hat{S}^{\dagger}, |0\rangle\langle 0|\right) = \frac{2\sinh(r/2)}{\sqrt{\cosh r}} \simeq 0 \end{aligned}$$

- Norm convexity,

$$d_{HS}\left(\mathbb{1}_b, \Gamma_N^{\xi}\right) \leq d_{HS}\left(\mathbb{1}_b, \Gamma_N\right) + d_{HS}\left(\Gamma_N^{\xi}, \Gamma_N\right) \simeq d_{HS}\left(\mathbb{1}_b, \Gamma_N\right) \tag{10}$$

- Brádler's result (Theorem 1) □

Conclusion

- Our squeezed GPQC well represents the dependance of the displacement and the squeezing elements, $\exp\left[-r_p^2\{1-\tanh r\cdot\cos(2\theta_{pq}-\phi)\}\right]$ whereas Brádler's CVPQC only depends on $\exp(-r_p^2)$ term of a coherent state.

- For sufficiently large N, the squeezed GPQC is *secure*:

$$d_{HS}\left(\mathbb{1}_b^{(\beta,\xi)},\mathcal{N}_N(\xi,|\beta\rangle\langle\beta|)\right)=d_{HS}\left(\mathbb{1}_b,\Gamma_N^{\xi}\right)\simeq d_{HS}\left(\mathbb{1}_b,\Gamma_N\right)\approx\sqrt{N^{-2}+O(N^{-4})}$$

  - Open question: In CV, $d_p\left(\rho_{thermal},\Gamma_N\right)\ll 1$?

  - **Acknowledgement**: This work was supported by the IT R&D program of MOTIE/KEIT [10043464]. SYL acknowledges support from FQXI and the National Research Foundation and Ministry of Education in Singapore.

Thank you for your attention !