Journal of Quantum Information Science, 2014, 4, 64-70
Published Online March 2014 in SciRes. http://www.scirp.org/journal/jqis
http://dx.doi.org/10.4236/jqis.2014.41006

Approximate Quantum State Sharings via Pair of Private Quantum Channels

Dong Pyo Chi[1], Kabgyun Jeong[2]

[1]Department of Mathematical Sciences, Seoul National University, Seoul, Korea
[2]School of Computational Sciences, Korea Institute for Advanced Study, Seoul, Korea
Email: kgjeong6@kias.re.kr

Received 13 January 2014; revised 22 February 2014; accepted 12 March 2014

Abstract

We investigate a quantum communication protocol, of so-called approximate quantum state sharing (AQSS), that protocol is basically based on pair of private quantum channels. In this paper, we prove that the scheme is secure against any external and internal attacks of wiretapping in principle. Although the protocol leaks small amount of information corresponding to a security parameter ε, the scheme still preserves its information-theoretic security.

Keywords

Quantum State Sharing; (Approximate) Private Quantum Channel; Trace Norm

1. Introduction

Quantum physics promises perfect and well-defined randomness, in this way, most of all quantum information-theoretic primitives try to offer an unconditional security given by the quantum randomness. For examples, quantum key distribution protocols such as BB84 [1] and B92 [2] highly depend on prerequisite random measurements, assigning randomness, for some quantum states.

Instead of such random measurements on quantum states, we can consider a direct randomizing technique for quantum encodings through a quantum channel. (Mathematically quantum channel is a completely positive and trance-preserving map.) These randomizing procedures can be efficiently accomplished by exploiting the notion of private quantum channel (PQC) or quantum one-time pad [3]. In the paper, we are interesting to special scheme of an *approximate* version of encryption/decryption, although it is not perfect but we can make use of the protocol to attempt to reduce some quantum operation resources. We also call the map to randomizing quantum states as random unitary channel (RUC) in the sense of quantum channel. In the future, we will use the meaning of private quantum channel as equivalent as random unitary channel. There are several methods for

How to cite this paper: Chi, D.P. and Jeong, K. (2014) Approximate Quantum State Sharings via Pair of Private Quantum Channels. *Journal of Quantum Information Science*, **4**, 64-70. http://dx.doi.org/10.4236/jqis.2014.41006

approximate randomizing quantum states, for examples, [4]-[6]. We here adapt the encoding/decoding logic of the work of Hayden *et al*. [4], and use the proof of Dickinson and Nayak's trace norm method [6]. There are many applications of the private quantum channel in quantum information science [4] [7] [8] and it is mostly originated from the approximate version of PQC.

In this paper, we propose an approximate quantum state sharing (AQSS) scheme in which participants use two parallel approximate private quantum channels (APQC). The scheme reduces a secret and random string (classical pre-shared key) of about one-half as compare to the complete PQC protocol. Actually our protocol naturally includes the famous quantum secret sharing protocols [9] [10] in broad sense. Furthermore, quantum states in itself are able to operate some quantum tasks, though those are not possible in classical regime. Assume that if there is a quantum computer only activated by a bipartite quantum state (or bipartite *quantum key*), then our protocol AQSS may achieve the goal efficiently, and also offers new opportunities for quantum information processing.

We briefly review the key-sharing efficiency of AQSS for using pair of random unitary channels. Assume that (a sender) Charlie prepares a pure quantum state φ_{AB} (two-qudit) and transmits the state to another distant receivers Alice and Bob through two independent RUCs. The transmitted state is generally maximally-mixed state. Then, for the state φ_{AB}, perfect randomization protocol requires exactly the amount of $4\log d$ -bits of unitary operations ($2\log d$ -bits for Alice and Bob, respectively), where d is the dimension of the input quantum state $\rho_{A(B)} := tr_{B(A)}\varphi_{AB}$ through each random unitary channels. On the other hand, the construction of Hayden *et al*.' method [4] for a pair of random unitary channels implies that only $2\log d + o(\log d)$-bits of unitaries are sufficient. In other words, perfect quantum state sharing (QSS) protocol by using bilateral PQCs needs to $4\log d$ -bits of shared secret information, while the approximate QSS protocol (by using bilateral PQCs) demands about only $2\log d$ bits of classical information. Note that the works in [5] [6] give a similar result, but the lower bound for the key-information is little bit improved.

After an introduction to the definition of random unitary channel, we shortly mention about special properties of a destruction of quantum states in Section 2. Main part follows in Section 3. In Section 3, we present our AQSS protocol based on two approximate PQCs, and investigate the information-theoretic security of AQSS under considering two attacks such as exterior and interior strategies, respectively. We finally conclude our results in Section 4.

2. Random Unitary Channel and Its Properties

Now we define random unitary channel (or private quantum channel), and then explicitly construct the approximate version of private quantum channel. For any density matrices $\varphi \in \mathfrak{B}(\mathbb{C}^d)$, a completely positive and trace-preserving map $N : \mathfrak{B}(\mathbb{C}^d) \to \mathfrak{B}(\mathbb{C}^d)$ is said to be ε *-randomizing*, if

$$\left\| N(\varphi) - \frac{\mathbb{I}}{d} \right\|_1 \le \varepsilon, \tag{1}$$

where the trace norm is defined by $\|X\|_1 = tr\sqrt{X^\dagger X}$, and $\mathfrak{B}(\mathbb{C}^d)$ denotes the bounded linear operator on d-dimensional (complex) Hilbert space $\mathbb{C}^d$. The character $\mathbb{I}$ represents the $d \times d$ identity matrix on the space. This definition directly induces the notion of the RUC or PQC. That is, for every $\varphi \in \mathfrak{B}(\mathbb{C}^d)$, a quantum channel $N : \mathfrak{B}(\mathbb{C}^d) \to \mathfrak{B}(\mathbb{C}^d)$ is called to private quantum channel, if the following construction

$$N(\varphi) = \sum_{i=1}^{n} p_i U_i \varphi U_i^\dagger \tag{2}$$

is ε -randomizing, where the unitary operator U_i live in a unitary group $\mathfrak{U}(d) \subset \mathfrak{B}(\mathbb{C}^d)$, and the probability p_i's are all positive and $\sum_i p_i = 1$. Notice that the parameter n is closely related to the number of Kraus (operation) elements for establishing the private quantum channel. The perfect PQC demands on exactly $n = d^2$ and this optimality condition is proved by several groups [11] [12].

For the approximate constructions of PQC, it was known that for all $\varepsilon > 0$ there exist a private quantum channel, in sufficiently larger dimension d, such that n can be taken to be $O(d\log d/\varepsilon^2)$ in [4] and $O(d/\varepsilon^2)$ in [13] where U_i's are chosen randomly according to the unitarily invariant measure (or Haar measure). We here fix the number n of having exactly $n = 150d/\varepsilon^2$ from the Theorem 1 in [13]. As mentioned in Introduction, most applications of private quantum channel are closely connected to the approximate version of the private quantum channel [4]. That is, approximate PQC is the main tool for constructing following

AQSS protocol.

The security of PQC is conserved by the argument of the accessible information in which leakage information is less than sufficiently small $\varepsilon > 0$. Although small leakage-information can be attacked to an eavesdropper (Eve), the Bob's decoding state is almost equal to the Alice's original state φ. **Figure 1** describes the total procedure of PQC. (The double line describes a classical channel for secret bits between Alice and Bob.)

Bilateral Private Quantum Channel

In this subsection we introduce a bilateral form of private quantum channels. These channels will be used to create following (approximate) QSS scheme in Section 3. First of all, we consider that two one-way independent PQCs are constituted between a sender Charlie and a receiver Alice, and Charlie and another receiver Bob, simultaneously. Then, let us define two PQCs, following the definition of Equation (2), such that

$$N_A(\varphi)=\frac{1}{n_A}\sum_{i=1}^{n_A}U_i\varphi U_i^{\dagger} \quad \text{and} \quad N_B(\varphi)=\frac{1}{n_B}\sum_{j=1}^{n_B}U_j\varphi U_j^{\dagger} \tag{3}$$

are ε-randomizing maps, where we fix a probability as equally weighted probabilities $p_i = 1/n_A$ and $p_j = 1/n_B$ for all i, j. For convenience, the number of n_A is fixed exactly equal to n_B, *i.e.*, $n_A = n_B = \frac{150d}{\varepsilon^2}$. As mentioned above, for an approximate, but secure, state sharing of any bipartite quantum states (either separable or entangled), those two channels play an important role to making approximate quantum state sharing scheme later.

For given N_A and N_B, and for all input $\varphi_{AB} \in \mathfrak{B}\left(\mathbb{C}^{d^2}\right)$, we can bound the trace norm for the difference between a channel-output state of product channel $N_A \otimes N_B$ and the maximally mixed state $\mathbb{I}/d^2$, such that

$$\left\| \left(N_A \otimes N_B\right)\left(\varphi_{AB}\right) - \frac{\mathbb{I}_A \otimes \mathbb{I}_B}{d^2} \right\|_1 \le \varepsilon, \tag{4}$$

where a security parameter ε is small and positive, but less than 1. The inequality above asserts that all encoding states are information-theoretically secure. Unfortunately, for any entangled state φ_{AB}, calculation of the bound is not a trivial task.

Here we notice that the efficiency argument for the randomizing procedure is intimately related to the destruction of correlations in the quantum states [4] [14]. Another words, if we desire to completely destroy the total correlation in the channel-output states, then we are needed to unitary operations of the amount of corresponding to the quantum mutual information $I[A:B] = S[\varphi_A] + S[\varphi_B] - S[\varphi_{AB}]$, where $S[\rho] = -tr\rho\log\rho$ the von Neumann entropy for given quantum state ρ. For example, a maximally entangled state $\varphi_{AB} = \frac{1}{d}\Sigma_{i,j}|ii\rangle_{AB}\langle jj|$ has precisely $I[A:B] = 2\log d$, so we guess the asymptotic amount of quantum operations needed. Formally speaking, the Equation (4), can be inferred from triangle inequality with respect to the

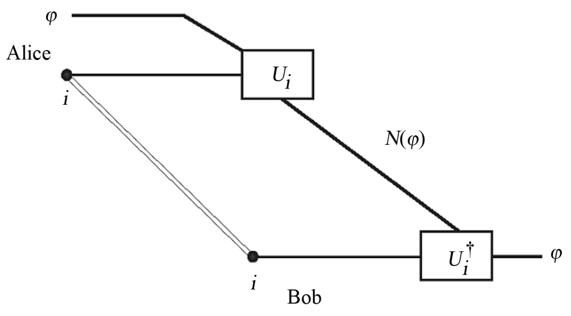

Figure 1. Private quantum channel: Alice applies U_i's for encoding of φ and Bob decodes $N(\varphi)$ with a secret key i which is pre-shared log n-bits of classical information.

trace norm on two PQCs, *i.e.*, suppose that $\left\| N_A(\varphi) - \frac{\mathbb{I}_A}{d} \right\|_1 \le \varepsilon$ and $\left\| N_B(\varphi) - \frac{\mathbb{I}_B}{d} \right\|_1 \le \varepsilon$, then we have $\left\| (N_A \otimes N_B)(\varphi_{AB}) - \mathbb{I}_{AB}/d^2 \right\|_1 \le 2\varepsilon$. (See the proof of the Proposition 1 in [14].) In Appendix of this paper, we examine the inequality precisely by exploiting the relation between the trace and Hilbert-Schmidt norms.

3. Approximate Quantum State Sharing Protocol

In this section we construct a scheme of so-called approximate quantum state sharing. Suppose that Charlie-Alice and Charlie-Bob are linked by independent two quantum communication channels of such approximate private quantum channels, which endow the outputs of d-dimensional maximally mixed states, respectively. First of all, Charlie prepares (arbitrary) bipartite quantum state $\varphi_{AB} \in \mathfrak{B}\left(\mathbb{C}^{d^2}\right)$, it does not matter the state of pure or mixed. He wants to securely transmit φ_{AB} to Alice and Bob together, and then to reconstruct the cleft state to original one on Alice and Bob's site via mutual cooperation. The total procedure of transmitting-reconstructing scheme, for a bipartite quantum state sharing, is quite simple, more specifically the scheme has only three steps:

- Sender Charlie prepares two-qudit φ_{AB}, and transmit the state through the channel $N_A \otimes N_B$ to two receivers Alice and Bob.
- Distant two parties Alice and Bob just hold the state they received, until they need the information of the quantum state.
- When Alice and Bob want to reveal the original state φ_{AB}, they must clearly cooperate in a single location. They perform inverse unitary operations based on the locally shared classical secret-key information.

The security check of the AQSS protocol is divided by two cases of exterior and interior attacks. Actually the security is based on information-theoretic assumption, which means that the intercepted states by Eve have sufficiently higher von Neumann entropy. Thus any attacks on the channel are impossible to be obtained any information to revealing the original quantum information.

First, let us take account of an attack accomplished by an external Eve. Suppose that if Eve intercepts the state $(N_A \otimes N_B)(\varphi_{AB})$, we hope that the state has higher entropic condition. In this reason, we propose that the entropy of the channel-output state to be following

$$S\left[(N_A \otimes N_B)(\varphi_{AB})\right] \approx 2\log d \to \infty \tag{5}$$

as d goes to infinity. (The notation "$\approx$" denotes that left side is "approximately equal to" right side.) We do not know the accurate description for the state $(N_A \otimes N_B)(\varphi_{AB})$ right now, so we divide the input state φ_{AB} into cases of separable and entangled, and prove its entropic condition. If product state is given, then it is possible to prove the inequality Equation (4) easily. Since, by using the triangle inequality once again with respect to the trace norm, the following inequality $\left\| (N_A \otimes N_B)(\varphi_{AB}) - \frac{\mathbb{I}_{AB}}{d^2} \right\|_1 \le 2\varepsilon$ holds for any $\varphi_{AB} = \varphi_A \otimes \varphi_B$. If we generally assume that $\varphi_{AB} = \sum_i p_i \varphi_{A,i} \otimes \varphi_{B,i}$ a separable state, then we have

$$\begin{aligned} \left\| (N_A \otimes N_B)(\varphi_{AB}) - \frac{\mathbb{I}_{AB}}{d^2} \right\|_1 &= \left\| \sum_{i=1}^{d} p_i N_A(\varphi_{A,i}) \otimes N_B(\varphi_{B,i}) - \frac{\mathbb{I}_{AB}}{d^2} \right\|_1 \\ &\le \sum_i p_i \left\| N_A(\varphi_{A,i}) \otimes N_B(\varphi_{B,i}) - \frac{\mathbb{I}_{AB}}{d^2} \right\|_1 \qquad (6) \\ &\le \sum_i p_i \left[\left\| N_A(\varphi_{A,i}) - \frac{\mathbb{I}_A}{d^2} \right\|_1 + \left\| N_B(\varphi_{B,i}) - \frac{\mathbb{I}_B}{d^2} \right\|_1 \right] \qquad (7) \\ &\le 2\varepsilon, \end{aligned}$$

where the inequalities Equations (6) and (7) are derived from the norm convexity and triangle inequality, respectively. Thus any separable inputs for the product channel are very close to the maximally mixed state $\mathbb{I}/d^2$. This implies that $S\left[(N_A \otimes N_B)(\varphi_{AB})\right]$ is equal to $2\log d$.

For the separable input cases, there is another proof that depends on the dimension parameter d and n: We can prove that the expectation value for the difference between the output of the quantum channel and the maximally mixed state (with respect to the trace norm) is bounded by a small quantity (dimension related)

$$\mathbb{E}\left\|\left(N_A \otimes N_B\right)\left(\varphi_{AB}\right)-\frac{\mathbb{I}}{d^2}\right\|_1 \leq \sqrt{\frac{d^2}{n_A \cdot n_B}}, \tag{8}$$

where $\mathbb{E} := \mathbb{E}_{\{U_{i,j}\}}$ denotes the total expectation of $\{U_i\}_{i=1}^{n_A}$ and $\{U_j\}_{j=1}^{n_B}$ for the independent PQCs N_A and N_B, respectively. The Appendix in this paper shows that the inequality Equation (8) can be derived precisely by exploiting the relation between the trace norm and Hilbert-Schmidt norm. As mentioned above, when one takes $n_A = 150d/\varepsilon^2$ and $n_B = 150d/\varepsilon^2$, then we have

$$\sqrt{\frac{d^2}{n_A \cdot n_B}} = \frac{\varepsilon^2}{150} < \varepsilon. \tag{9}$$

This implies that Eve's attack is impossible in principle. Then how can we treat of entangled input states? Although direct proof is impossible, there is an evidence for the statement on Equation (5). The Theorem III.3 in [4] states that, for a positive operator-valued measure (POVM) $\{L_i\}$ which is implemented by using local operation and classical communication (LOCC),

$\sum_i \left\|p_i - q_i\right\|_1 \leq \varepsilon$ is true, where $p_i := tr\left(L_i\left(N_A \otimes \mathbb{I}_B\right)\left(\varphi_{AB}\right)\right)$ and $q_i := tr\left(L_i\left(\frac{\mathbb{I}_A}{d} \otimes \varphi_B\right)\right)$ with a maximally entangled state such that $\varphi_{AB} = \frac{1}{d}\sum_{i,j}^{d}\left|ii\right\rangle_{AB}\left\langle jj\right|$ and $\varphi_B = tr_A \varphi_{AB}$. Natural extension to channel B is possible via adding the channel N_B: Define $p_i = tr\left(L_i\left(N_A \otimes N_B\right)\left(\varphi_{AB}\right)\right)$ and $q_i = tr\left(L_i\left(\frac{\mathbb{I}_{AB}}{d^2}\right)\right)$, then also we have $\sum_i \left\|p_i - q_i\right\|_1 \leq \varepsilon$ Therefore, we can conclude that an output state of the product channel, $\left(N_A \otimes N_B\right)\left(\varphi_{AB}\right)$, is close to $\mathbb{I}/d^2$ under the LOCC-implemented POVM. In this reason, any input entangled states φ_{AB} through the product channel $N_A \otimes N_B$ has always high entropy condition for $d \gg 1$.

Second, we take care of a situation when Alice or Bob is malicious. Assume that Bob intercepts the Alice's state $N_A\left(\varphi_A\right)$, but Bob's state decoded will be

$$\left(\mathbb{I}_A \otimes N_B^*\right)\left(N_A \otimes N_B\right)\left(\varphi_{AB}\right) = \left(N_A \otimes \mathbb{I}_B\right)\left(\varphi_{AB}\right), \tag{10}$$

where * denotes the inverse (unitary) operation for Bob's PQC N_B, so $S\left[N_A\left(\varphi_A\right)\right]$ for the resulting state has still higher entropy such as $\log d$. Because the intercepted state $tr_B\left(\left(N_A \otimes N_B\right)\left(\varphi_{AB}\right)\right)$ is almost maximally mixed state by the definition of PQC $N_A\left(\varphi_A\right)$. Thus, Bob cannot obtain any information for φ_A without Alice's secret key information. Symmetrically, Alice's attack is also useless. In other words, Charlie's aim of sharing a quantum state φ_{AB} between Alice and Bob can be securely accomplished. At least two attacks of external and internal eavesdroppings cannot break the security condition of our AQSS protocol. Furthermore, only cooperation between Alice and Bob always gives birth to the original state.

We notice that perfect protocol for QSS requires exactly d^4 unitary operators as mentioned above, while our protocol is only needed to total $22500d^2/\varepsilon^4$ unitaries. This fact directly implies that some shared key bits can be reduced about $1/2$. Because our AQSS is just needed $2\log d - 4\log\varepsilon + O(1)$ secret bits, but perfect QSS is required $4\log d$ bits. In summary of this section, for any state $\varphi_{AB} \in \mathfrak{B}\left(\mathbb{C}^{d^2}\right)$ and a quantum channel N_{AB} (for an $\varepsilon' > 0$ is arbitrary), assume that following inequality

$$\left\|N_{AB}\left(\varphi_{AB}\right)-\frac{\mathbb{I}}{d^2}\right\|_1 \leq \varepsilon'. \tag{11}$$

Then, it is sufficient to create a perfect QSS $\left(\varepsilon' = 0\right)$ with d^4 unitary operations [4] [6]. In the case, our approximate QSS via pair of two PQCs, $N_{AB} = N_A \otimes N_B$, just consume of one-half secret classical bits. Thus we can say that it is efficient.

Finally we remark that a direct generalization is possible for the bipartite quantum state sharing (Equation (8)) scheme to a multiparty approximate quantum state sharing (MAQSS), and the secrecy is also preserved. Suppose that a situation of Charlie (C) prepares an m-qudit quantum state $\varphi_{A_1A_2\cdots A_m}$. If they had secret bitstrings for PQCs between $C\text{-}A_1$, $C\text{-}A_2$ and so on, then we have

$$\left\| \left(N_{A_1} \otimes N_{A_2} \otimes \cdots \otimes N_{A_m}\right)\left(\varphi_{A_1 A_2 \cdots A_m}\right) - \frac{\mathbb{I}}{d^m} \right\|_1 \leq \varepsilon. \tag{12}$$

Equation (12) implies that any exterior attacks are failed, as well as all interior attacks (including group conspiracy) are also to be frustrated, since, without secret-bits of another participants, it is similar to the two receiver cases. We briefly mention about the cost of secret classical information on MAQSS scheme. Roughly speaking, the perfect scheme requires $2m\log d$ classical bits, but the MAQSS only $m\log d + o(\log d)$-bits are sufficient. As an alternative of the study on multiparty AQSS protocol, in the near future we will analyze that a generalized security proof of AQSS with respect to the Shatten p-norms beyond the trace case.

4. Conclusion

We studied that an approximate quantum state sharing scheme is efficient from the classical information cost of view and the protocol is robust to the two kinds (internal and external) of wiretappings from the construction via bilateral private quantum channel. Especially, we analyzed that given protocol is strong under the channel-inputs of all separable and entangled quantum states. The proposed AQSS protocol basically depends on approximate private quantum channels, which are essentially equivalent to pair of independent random unitary channels. Although the protocol leaks small information corresponding to a security parameter ε, we can conclude that the scheme preserves its information-theoretic security for any bipartite quantum states.

Acknowledgements

This work was partly supported by the IT R\&D program of MOTIE/KEIT [10043464 (2013)].

References

[1] Bennett, C.H. and Brassard, G. (1984) Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, 175-179.

[2] Bennett, C.H. (1992) Quantum Cryptography Using Any Two Nonorthogonal States. *Physical Review Letters*, **68**, 3121. http://dx.doi.org/10.1103/PhysRevLett.68.3121

[3] Ambainis, A., Mosca, M., Tapp, A. and de Wolf, R. (2000) Private Quantum Channels. *IEEE Symposium on Foundations of Computer Sciences* (*FOCS*), 547-553.

[4] Hayden, P., Leung, D., Shor, P.W. and Winter, A. (2004) Randomizing Quantum States: Constructions and Applications. *Communication in Mathematical Physics*, **250**, 371-391. http://dx.doi.org/10.1007%2Fs00220-004-1087-6

[5] Ambainis, A. and Smith, A. (2004) Small Pseudo-Random Families of Matrices: Derandomizing Approximate Quantum Encryption. *Proceedings of RANDOM*, LNCS 3122, Springer, Berlin-Heidelberg-New York.

[6] Dickinson, P.A. and Nayak, A. (2006) Approximate Randomization of Quantum States With Fewer Bits of Key. *AIP Conference Proceedings*, **864**, 18. http://dx.doi.org/10.1063/1.2400876

[7] Harrow, A., Hayden, P. and Leung, D. (2004) Superdense Coding of Quantum States. *Physical Review Letters*, **92**, Article ID: 187901. http://dx.doi.org/10.1103/PhysRevLett.92.187901

[8] Bennett, C.H., Hayden, P., Leung, D., Shor, P.W. and Winter, A. (2006) Remote Preparation of Quantum States. *IEEE Transactions on Information Theory*, **51**, 56-74. http://dx.doi.org/10.1109/TIT.2004.839476

[9] Hillery, M., Bužek, V. and Berthiaume, A. (1999) Quantum Secret Sharing. *Physical Review A*, **59**, 1829. http://dx.doi.org/10.1103/PhysRevA.59.1829

[10] Karlsson, A., Koashi, M. and Imoto, N. (1999) Quantum Entanglement for Secret Sharing and Secret Splitting. *Physical Review A*, **59**, 162. http://dx.doi.org/10.1103/PhysRevA.59.162

[11] Nagaj, D. and Kerenidis, I. (2006) On the Optimality of Quantum Encryption Schemes. *Journal of Mathematical Physics*, **47**, Article ID: 092102. http://dx.doi.org/10.1063/1.2339014

[12] Bouda, J. and Ziman, M. (2007) Optimality of Private Quantum Channels. *Journal of Physics A*: *Mathematical and Theoretical*, **40**, 5415. http://dx.doi.org/10.1088/1751-8113/40/20/011

[13] Aubrun, G. (2009) On Almost Randomizing Channels with a Short Kraus Decomposition. *Communication in Mathematical Physics*, **288**, 1103-1116. http://dx.doi.org/10.1007/s00220-008-0695-y

[14] Groisman, B., Popescu, S. and Winter, A. (2005) Quantum, Classical, and Total Amount of Correlations in a Quantum state. *Physical Review A*, **72**, Article ID: 032317. http://dx.doi.org/10.1103/PhysRevA.72.032317

Appendix

For given two random unitary channels $N_A(\varphi_A)$ and $N_B(\varphi_B)$ in Equation (3), and for all pure separable states $\varphi_{AB} \in \mathfrak{B}\left(\mathbb{C}^{d^2}\right)$,

$$\begin{aligned}\left\|(N_A \otimes N_B)(\varphi_{AB})\right\|_2^2 = tr\left[(N_A \otimes N_B)(\varphi_{AB})\right]^2 &= \frac{1}{n_A^2 n_B^2}\sum_{i=1}^{n_A}\sum_{j=1}^{n_B} tr\left(U_i \otimes U_j \varphi_{AB} U_i^\dagger \otimes U_j^\dagger\right)^2 \\ &+ \frac{1}{n_A^2 n_B^2}\sum_{i\neq k}^{n_A}\sum_{j\neq l}^{n_B} tr\left(U_i \otimes U_j \varphi_{AB} U_i^\dagger \otimes U_j^\dagger\right)\left(U_k \otimes U_l \varphi_{AB} U_k^\dagger \otimes U_l^\dagger\right)\end{aligned} \tag{13}$$

where $tr\left(U_i \otimes U_j \varphi_{AB} U_i^\dagger \otimes U_j^\dagger\right)^2$ for any pure state φ_{AB}. (Note that this method is just an expansion of the statement, the chapter 3, in [8].)

Recall that the unitary operators are chosen randomly according to the unitarily invariant (Haar) measure, and if we take the expectation over all random selection of unitaries, then

$$\mathbb{E}_{\{U_{i,j}\}}\left[tr\left((N_A \otimes N_B)(\varphi_{AB})\right)^2\right] = \frac{1}{n_A n_B} + \frac{1}{n_A^2 n_B^2}\sum_{i\neq k}^{n_A}\sum_{j\neq l}^{n_B} tr\left(U_i \otimes U_j \varphi_{AB} U_i^\dagger \otimes U_j^\dagger\right)\left(U_k \otimes U_l \varphi_{AB} U_k^\dagger \otimes U_l^\dagger\right)$$

$$= \frac{1}{n_A n_B} + tr\left[\mathbb{E}_{\{U_{i,j}\}}\left(U_i \otimes U_j \varphi_{AB} U_i^\dagger \otimes U_j^\dagger\right)\mathbb{E}_{\{U_{k,l}\}}\left(U_k \otimes U_l \varphi_{AB} U_k^\dagger \otimes U_l^\dagger\right)\right] \tag{14}$$

$$= \frac{1}{n_A n_B} + tr\frac{\mathbb{I}}{d^4} \tag{15}$$

$$= \frac{1}{n_A n_B} + \frac{1}{d^2}. \tag{16}$$

In Equation (14), we make use of the fact that the sets of unitary operators $U_{i,j}$ and $U_{k,l}$ are chosen independently at random, and the Equation (15) is inherited from the definition of the Haar measure on the unitary group. (Notice that for any $\varphi \in \mathfrak{B}\left(\mathbb{C}^d\right)$, a Haar-distributed unitary set $U := \{U_i\}_{i=1}^n \subset \mathfrak{U}(d)$ satisfies that $\mathbb{E}_U U\varphi U^\dagger = \int U\varphi U^\dagger \mathrm{d}U = \frac{\mathbb{I}}{d}$.) The Equation (15) exploits the separable condition for φ_{AB}. Note that, for any rank d matrix X, $\|X\|_1 \le \sqrt{d}\,\|X\|_2$, actually it is the very Cauchy-Schwartz inequality. For any rank d^2 matrix X, a generalization of the Corollary A.2 in [8] directly shows that

$$\left\|X - \frac{\mathbb{I}_A \otimes \mathbb{I}_B}{d^2}\right\|_1^2 \le d^2\|X\|_2^2 - 1. \tag{17}$$

Then, from considering the random variable Y defined by $Y = \left\|(N_A \otimes N_B)(\varphi_{AB}) - \frac{\mathbb{I}}{d^2}\right\|_1$ and by using Equation (16), we have

$$\mathbb{E}Y \le \sqrt{\mathbb{E}Y^2} \le \sqrt{d^2\|Y\|_2^2 - 1} = \sqrt{\frac{d^2}{n_A \cdot n_B}}. \tag{18}$$