Capacity of Quantum Private Information Retrieval with Colluding Servers

Seunghoan Song[1] * Masahito Hayashi[2 1] †

[1]*Graduate School of Mathematics, Nagoya University, Nagoya, Japan*
[2]*Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen, China*

A full version of this paper is accessible at: `https://arxiv.org/pdf/2001.04436.pdf`.

When a user retrieves information from databases, it is often required to protect the privacy of the user. Private information retrieval (PIR) is a protocol in which a user retrieves one of multiple messages from server(s) without revealing which message is retrieved to any individual server. The optimal solution of single-server PIR is downloading all messages in the server [1] but this solution is inefficient. To improve communication efficiency, multi-server PIR has been studied with the assumption that the servers cannot communicate with each other. Symmetric PIR [2] is multi-server PIR with servers' secrecy in which the user only obtains the retrieved message but no other information of other messages. Quantum PIR (QPIR) has been studied [3–12] for retrieving a classical message with quantum communication.

Our previous paper [10] investigated the fundamental communication limit of symmetric and non-symmetric multi-server QPIR and constructed an optimal protocol achieving the communication limit. The paper [10] considered the communication model in which the user sends classical query and the servers return quantum answers but the servers share prior entanglement before the protocol starts. The communication efficiency of a QPIR protocol is evaluated by the *QPIR rate* defined as the ratio of the one message size to the whole dimension of the downloaded quantum systems. Higher QPIR rate implies higher communication efficiency and an upper bound of QPIR rates is 1 from definition. The maximum of QPIR rates, called the *QPIR capacity*, characterizes the optimal communication efficiency of QPIR. The paper [10] proved that the symmetric and non-symmetric QPIR capacities are 1. Capacity 1 implies that symmetric QPIR can be achieved with the same efficiency as retrieval without secrecy.

However, the multi-server model considered in [10] has a critical weakness that the assumption of no communication among servers is too restrictive. By relieving this assumption, t-*private QPIR* is QPIR in which the identity of the retrieved message is kept secret even if at most t servers may communicate and collude. In this paper, we study t-private QPIR capacity. Under the same communication model as [10], we prove that the symmetric and non-symmetric t-private n-server QPIR capacities C_{t} are both

$$C_{\mathsf{t}} = \begin{cases} 1 & \text{if } 1 \le \mathsf{t} \le \frac{\mathsf{n}}{2} \\ \frac{2(\mathsf{n}-\mathsf{t})}{\mathsf{n}} & \text{if } \frac{\mathsf{n}}{2} < \mathsf{t} \le \mathsf{n}-1 \end{cases}. \tag{1}$$

Our result implies that even if some servers collude, as far as the number of colluding servers is less than half ($\mathsf{t} \le \frac{\mathsf{n}}{2}$), the remarkable result of QPIR capacity 1 still applies to the t-private case, i.e., symmetric t-private QPIR can be achieved with the same efficiency as retrieval without secrecy. Our result includes the capacity in [10] as the case $\mathsf{t} = 1$. As in Table 1, the t-private QPIR capacity is greater than the classical counterparts.

The proof of (1) consists of two parts. First, we construct an optimal symmetric t-private QPIR protocol by the stabilizer formalism. Second, we derive the tight upper bound of C_{t} by the capacity of entanglement-assisted classical-quantum channel coding [17] since we can reduce t-private QPIR protocols to the latter problem [17] by QPIR's secrecy.

Table 1: Classical and quantum PIR Capacities

	Classical PIR Capacity	Quantum PIR Capacity
PIR	$\frac{1-\mathsf{n}^{-1}}{1-\mathsf{n}^{-\mathsf{f}}}$ [13]	1 [10]
Symmetric PIR	$1-\frac{1}{\mathsf{n}}$ [14]	1 [10]
t-Private PIR	$\frac{1-\mathsf{t}/\mathsf{n}}{1-(\mathsf{t}/\mathsf{n})^{\mathsf{f}}}$ [15]	$\min\left\{1, \frac{2(\mathsf{n}-\mathsf{t})}{\mathsf{n}}\right\}$ [This paper]
t-Private symmetric PIR	$\frac{\mathsf{n}-\mathsf{t}}{\mathsf{n}}$ [16]	

∗ n, f: the numbers of servers and files, respectively.

*m17021a@math.nagoya-u.ac.jp
†hayashi@sustech.edu.cn

References

[1] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," *Journal of the ACM,* 45(6):965–981, 1998.

[2] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin. "Protecting data privacy in private information retrieval schemes," *Journal of Computer and Systems Sciences*, 60(3):592–629, 2000. Earlier version in STOC 98.

[3] I. Kerenidis and R. de Wolf. "Exponential lower bound for 2-query locally decodable codes via a quantum argument," *Proceedings of 35th ACM STOC*, pp. 106–115, 2003.

[4] I. Kerenidis and R. de Wolf, "Quantum symmetrically-private information retrieval," *Information Processing Letters*, vol. 90, pp. 109–114, 2004.

[5] L. Olejnik, "Secure quantum private information retrieval using phase-encoded queries," *Physical Review A* 84, 022313, 2011.

[6] F. Le Gall, "Quantum Private Information Retrieval with Sublinear Communication Complexity," *Theory of Computing*, 8(16):369–374, 2012.

[7] Ä. Baumeler and A. Broadbent, "Quantum Private Information Retrieval has linear communication complexity," *Journal of Cryptology*, vol. 28, issue 1, pp. 161–175, 2015.

[8] I. Kerenidis, M. Laurière, F. Le Gall, and M. Rennela, "Information cost of quantum communication protocols," *Quantum information & computation,* 16(3-4):181–196, 2016.

[9] D. Aharonov, Z. Brakerski, K.-M. Chung, A. Green, C.-Y. Lai, O. Sattath, "On Quantum Advantage in Information Theoretic Single-Server PIR," *In: Ishai Y., Rijmen V. (eds) EUROCRYPT 2019,* Springer, Cham, vol. 11478, 2019.

[10] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Multiple Servers," *IEEE Transactions on Information Theory*, DOI:10.1109/TIT.2020.3022515, in press.

[11] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Collusion of All But One of Servers," *Proceedings of 2019 IEEE Information Theory Workshop (ITW)*, pp. 1–5, 2019.

[12] M. Allaix, L. Holzbaur, T. Pllaha, and C. Hollanti, "Quantum Private Information Retrieval from MDS-coded and Colluding Servers," *arXiv:2001.05883 [cs.IT]*, 2020.

[13] H. Sun and S. Jafar, "The capacity of private information retrieval," *IEEE Transactions on Information Theory*, vol. 63, no. 7, pp. 4075–4088, 2017.

[14] H. Sun and S. Jafar, "The Capacity of Symmetric Private Information Retrieval," 2016 IEEE Globecom Workshops (GC Wkshps), Washington, DC, 2016, pp. 1–5.

[15] H. Sun and S. Jafar, "The capacity of robust private information retrieval with colluding databases," *IEEE Transactions on Information Theory*, vol. 64, no. 4, pp. 2361–2370, 2018.

[16] Q. Wang and M. Skoglund, "Secure Symmetric Private Information Retrieval from Colluding Databases with Adversaries," *2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 1083–1090, 2017.

[17] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted classical capacity of noisy quantum channels," Physical Review Letters, 83(15):3081-3084, 1999.