

Seunghoan Song

JSPS Research Fellow PD
Graduate School of Mathematics, Nagoya University
seunghoans@gmail.com
August 12, 2021

About Me

My interests lie in the intersection of information theory, cryptography, and quantum information science. I use the tool of information theory and coding theory to find optimal structures in classical/quantum cryptography. I have particularly studied the following topics.

- private information retrieval with quantum resources
- equivalence between non-perfect secret sharing and symmetric private information retrieval
- secure quantum network communication

Personal Information

Nationality	Republic of Korea
Languages	Korean, English, Japanese
Homepage	https://www.math.nagoya-u.ac.jp/~m17021a/index.html

Research Positions

Jan.2021 - Present **JSPS Reserach Fellow PD**
Graduate Schools of Mathematics, Nagoya University, Japan

Education

Apr.2019 - Dec.2020 **PhD in Mathematical Science, Nagoya University, Japan**
Thesis: Information-Theoretic Aspects of Quantum Private Information Retrieval
Advisor: Masahito Hayashi and François Le Gall

Apr.2017 - Mar.2019 **Master of Mathematical Science, Nagoya University, Japan**
Graduation with "Graduate School of Mathematics Award for Masters Thesis"
Thesis: Secure Quantum Network Code
Advisor: Masahito Hayashi

Apr.2011 - Mar.2017 **B.E. in Information and Computer Sciences, Osaka University, Japan**
Graduation with top honors at department
Thesis: Sphere Packing Bound and Gilbert-Varshamov Bound for b -Symbol Read Channels
Advisor: Toru Fujiwara
(Leave of absence due to military service obligation: 2014-2015)

Honors and Awards

Research Grant

Apr.2020 - Mar.2022 JSPS Grant-in-Aid for JSPS Fellows No. JP20J11484.
Project: Security and Efficiency Analysis of Quantum Private Information Retrieval and Quantum Oblivious Transfer

Awards

Jun.2020 Student Presentation Award, 41st Quantum Information Technology Symposium (QIT41)
Mar.2019 Graduate School of Mathematics Award for Masters Thesis
Mar.2017 2017 School of Engineering Science Outstanding Student Award
Graduation with top honors at Software Science Course, Department of Information and Computer Sciences, School of Engineering Science, Osaka University.
Jan.2013 Osaka University General Education Curriculum Scholarships
Awarded to top 50 ranked second-year students in general education curriculum (Admission Quota of Osaka University: 3,255).

Scholarships

Apr.2020 - Mar.2022 JSPS Research Fellowships for Young Scientists
Oct.2019 - Mar.2020 Lotte Foundation Scholarship
Apr.2018 - Mar.2019 Rotary Yoneyama Memorial Master Course Scholarship
Apr.2017 - Mar.2018 Monbukagakusho Honors Scholarship for Privately-Financed International Students
Mar.2010 - Mar.2017 Korea-Japan Joint Government Scholarship for Students in Departments of Science and Engineering

Other Employments

Apr.2019 - Mar.2020 Research Assistant, Nagoya University
Principal Investigator: Prof. Masahito Hayashi.
Apr.2017 - Sep.2018 Teaching Assistant, Nagoya University
Linear Algebra (Course in Japanese), Spring-Fall 2017.
Linear Algebra (Course in English), Spring-Fall 2017 and Spring 2018.
Mar.2014 - Dec.2015 Republic of Korea Army (military service obligation)
Sep.2013 NS Solutions Corporation (system engineer internship)

Skills

Python, Matlab, Pytorch, R, Java, C.

Publications

I published 6 refereed journal papers and 7 refereed conference proceedings. Published journals include IEEE Transactions on Information Theory (premier journal in information theory) and Physical Review Research (leading journal in physics).

Peer-Reviewed Journal Papers

6. Seunghoan Song and Masahito Hayashi, “Capacity of Quantum Private Information Retrieval with Colluding Servers,” *IEEE Transactions on Information Theory*, vol. 67, no. 8, pp. 5491–5508, 2021.
5. Seunghoan Song and Masahito Hayashi, “Capacity of Quantum Private Information Retrieval with Collusion of All But One of Servers,” *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 380–390, 2021.
4. Seunghoan Song and Masahito Hayashi, “Capacity of Quantum Private Information Retrieval with Multiple Servers,” *IEEE Transactions on Information Theory*, vol. 67, no. 1, pp. 452–463, 2021.
3. Masahito Hayashi and Seunghoan Song, “Quantum state transmission over partially corrupted quantum information network,” *Physical Review Research*, 2, 033079, 2020.
2. Seunghoan Song and Masahito Hayashi, “Secure Quantum Network Code without Classical Communication,” *IEEE Transactions on Information Theory*, vol. 66, no. 2, pp. 1178–1192, 2020.
1. Seunghoan Song and Toru Fujiwara, “Sphere Packing Bound and Gilbert-Varshamov Bound for b -Symbol Read Channels,” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E101-A, no.11, pp. 1915–1924, 2018.

Peer-Reviewed Conference Proceedings

7. Seunghoan Song and Masahito Hayashi, “Equivalence of Non-Perfect Secret Sharing and Symmetric Private Information Retrieval with General Access Structure,” *Proceedings of 2021 IEEE International Symposium on Information Theory (ISIT2021)*, in press. ([arXiv:2101.11194 \[cs.CR\]](https://arxiv.org/abs/2101.11194))
6. Seunghoan Song and Masahito Hayashi, “Quantum Private Information Retrieval for Quantum Messages,” *Proceedings of 2021 IEEE International Symposium on Information Theory (ISIT2021)*, in press. ([arXiv:2101.09041 \[quant-ph\]](https://arxiv.org/abs/2101.09041))
5. Seunghoan Song and Masahito Hayashi, “Capacity of Quantum Private Information Retrieval with Colluding Servers,” *Proceedings of 2020 IEEE International Symposium on Information Theory (ISIT2020)*, pp. 1727–1731, 2020.
4. Seunghoan Song and Masahito Hayashi, “Capacity of Quantum Private Information Retrieval with Collusion of All But One of Servers,” *Proceedings of 2019 IEEE Information Theory Workshop (ITW2019)*, pp. 1–5, 2019.
3. Seunghoan Song and Masahito Hayashi, “Capacity of Quantum Private Information Retrieval with Multiple Servers,” *Proceedings of 2019 IEEE International Symposium on Information Theory (ISIT2019)*, pp. 1727–1731, 2019.
2. Seunghoan Song and Masahito Hayashi, “Secure Quantum Network Code without Classical Communication,” *Proceedings of 2018 IEEE Information Theory Workshop (ITW2018)*, pp. 1–5, 2018.
1. Seunghoan Song and Masahito Hayashi, “Quantum Network Code for Multiple-Unicast Network with Quantum Invertible Linear Operations,” *Proceedings of 13th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC2018)*, vol. 111, pp. 10:1–10:20, 2018.

Preprints

1. *Matteo Allaix, *Seunghoan Song, Lukas Holzbaur, Tefjol Pllaha, Masahito Hayashi, Camilla Hollanti, “On the Capacity of Quantum Private Information Retrieval from MDS-Coded and Colluding Servers,” [arXiv:2106.14719 \[cs.IT\]](https://arxiv.org/abs/2106.14719), 2021. (* M. Allaix and S. Song are co-first authors.)

Talks

Refereed Conference Talks

IEEE International Symposium on Information Theory (**ISIT**) is the most prestigious event in information theory and IEEE Information Theory Workshop (**ITW**) is a leading workshop in information theory focused on selected topics. Conference on the Theory of Quantum Computation, Communication and Cryptography (**TQC**) and Asian Quantum Information Science Conference (**AQIS**) is leading conferences in quantum information science including quantum computation and cryptography. Beyond IID in Information Theory (**BeyondIID**) is a specialized workshop on quantum/classical information theory.

11. **ISIT2021** “Equivalence of Non-Perfect Secret Sharing and Symmetric Private Information Retrieval with General Access Structure,” Melbourne, Victoria, Australia (hosted online), July. 12–20, 2021.
10. **ISIT2021** “Quantum Private Information Retrieval for Quantum Messages,” Melbourne, Victoria, Australia (hosted online), July. 12–20, 2021.
9. **AQIS2020** “Capacity of Quantum Private Information Retrieval with Colluding Servers,” University of Technology Sydney, Sydney, Australia (hosted online), Dec. 7–9, 2020.
8. **BeyondIID8** “Capacity of Quantum Private Information Retrieval with Colluding Servers” (Lightning Talk), Stanford University, California, US (hosted online), Nov. 9–13, 2020.
7. **ISIT2020** “Capacity of Quantum Private Information Retrieval with Colluding Servers,” Los Angeles, California, USA (hosted online), Jun. 21–26, 2020.
6. **ITW2019** “Capacity of Quantum Private Information Retrieval with Collusion of All But One of Servers,” Donners Event, Visby, Sweden, Aug. 25–28, 2019.
5. **AQIS2019** “Capacity of Quantum Private Information Retrieval with Multiple Servers,” Korea Institute for Advanced Study, Seoul, Korea, Aug. 19–23, 2019.
4. **ISIT2019** “Capacity of Quantum Private Information Retrieval with Multiple Servers,” Maison de la Mutualite, Paris, France, Jul. 7–12, 2019.
3. **BeyondIID7** “Capacity of Quantum Private Information Retrieval with Multiple Servers,” University of Technology Sydney, Sydney, Australia, Jul. 1–5, 2019.
2. **ITW2018** “Secure Quantum Network Code without Classical Communication,” Sun Yat-sen University, Guangzhou, China, Nov. 25–29, 2018.
1. **TQC2018** “Quantum Network Code for Multiple-Unicast Network with Quantum Invertible Linear Operations,” University of Technology Sydney, Sydney, Australia, Jul. 16–18, 2018.

Invited Talks

4. “Secure quantum network code: universal construction and capacity,” SUSTech-Nagoya workshop on Quantum Science, Online, Jun. 21–24, 2021.
3. “Secure quantum network code: universal construction and capacity,” KIAS seminar, Korea Institute for Advanced Study (KIAS), Seoul, Korea, Aug. 9, 2019.
2. “Capacity of Quantum Private Information Retrieval with Multiple Servers,” Nagoya-SUSTech Quantum Information Workshop, Nagoya, Japan, Apr. 11–13, 2019.
1. “Secure Quantum Network Code without Classical Communication,” YITP seminar, Kyoto University, Kyoto, Japan, May 16, 2018.

Refereed Poster Presentations in International Meetings

6. “Capacity of Quantum Private Information Retrieval with Colluding Servers,” 24rd Annual Conference on Quantum Information Processing (QIP2021), Munich, Germany, Feb. 1–5, 2021.
5. “Capacity of Quantum Private Information Retrieval with Colluding Servers,” QCrypt2020, Online Conference, Aug. 10–14, 2020.

4. "Quantum State Transmission over Partially Corrupted Quantum Network," 23rd Annual Conference on Quantum Information Processing (QIP2020), Shenzhen, China, Jan. 6–10, 2020.
 3. "Capacity of Quantum Private Information Retrieval with Multiple Servers," 23rd Annual Conference on Quantum Information Processing (QIP2020), Shenzhen, China, Jan. 6–10, 2020.
 2. "Quantum Network Code for Multiple-Unicast Network with Quantum Invertible Linear Operations," 18th Asian Quantum Information Science Conference (AQIS2018), Nagoya, Japan, Sep. 8–12, 2018.
 1. "Secure Quantum Network Code without Classical Communication," 2018 IEEE International Symposium on Information Theory (ISIT2018), Colorado, U.S., Jun. 17–22, 2018.
-

Professional Service

Journal Referee IEEE Journal on Selected Areas in Information Theory (JSAIT),
IEEE Transactions on Computers (TCSI),
Entropy,
International Journal of Quantum Information (IJQI)

Conference Referee IEEE International Symposium on Information Theory (ISIT),
IEEE Information Theory Workshop (ITW)
