（別紙様式５）

変革を駆動する先端物理・数学プログラム（FoPM）

国外連携機関長期研修　報告書

氏　　名	松井　浩介
所属部局	理学系研究科　　物理学専攻
受入先	University of Edinburgh
日程	西暦 2026 年 2 月 6 日 ～ 西暦 2026 年 2 月 20 日

Overview

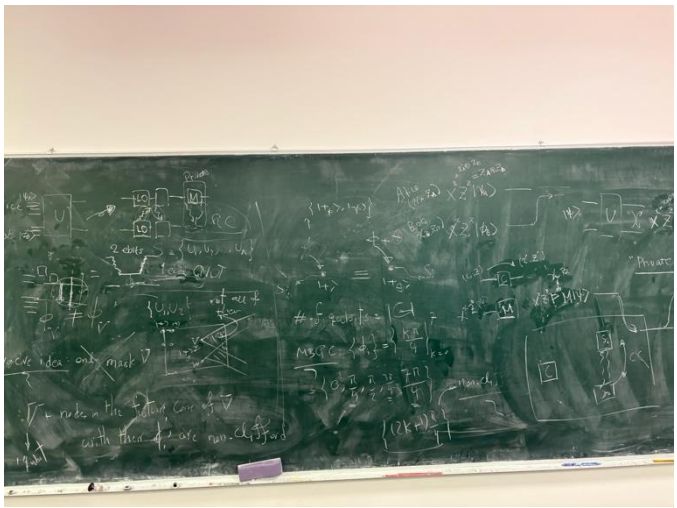
From February 6 to February 20, 2026, I stayed in Edinburgh, UK, and visited the School of Informatics at the University of Edinburgh. During this visit, I conducted collaborative research on two projects in quantum information theory: entanglement cost in secure two-party quantum computation, and distributed mixed-state tomography under communication constraints. I discussed the first project mainly with Assistant Professor Alexandru Cojocaru and postdoctoral researcher Dominik Leichtle, and the second project with Assistant Professor Mina Doosti and PhD student Chirag Wadhwa. The visit was organized mainly around detailed research discussions, which allowed me to examine both projects from several complementary viewpoints.

Research on secure two-party quantum computation

The first project concerned entanglement cost in secure two-party quantum computation. In this setting, two parties jointly implement a bipartite quantum operation while keeping each private input hidden from the other. My goal is to clarify how much quantum communication, or equivalently entanglement, is required for such secure implementations. Through discussions with Alexandru Cojocaru and Dominik Leichtle, I learned how this question relates to prior work in quantum cryptography and how to position my research more clearly within the existing literature.

They first introduced me to an important paper [1] showing that secure two-party quantum computation is possible for arbitrary unitaries against specious adversaries. This result establishes general feasibility, but it does not address entanglement cost, and its protocol does not seem to be optimized from the viewpoint of entanglement efficiency. This confirmed for me that my research question is meaningful: even if secure implementation is possible in principle, it remains important to understand how much entanglement is actually necessary. Our discussions also made clear that the quantum cryptography literature often emphasizes benchmarks that differ from those natural in distributed quantum computation, which helped me place my question more precisely.

We also discussed the possibility that, for Clifford unitaries, the additional entanglement cost caused by security requirements may be relatively small. After returning to Japan, I would like to examine more carefully whether this possibility can be established mathematically. Through discussions with PhD student Abbas Poshtvan, I also learned that a similar tendency toward low entanglement cost for Clifford unitaries appears in MBQC-based approaches. Understanding the relation between our approach and MBQC-based approaches therefore seems especially interesting.



Picture 1. Discussion during the visit on secure two-party quantum computation.

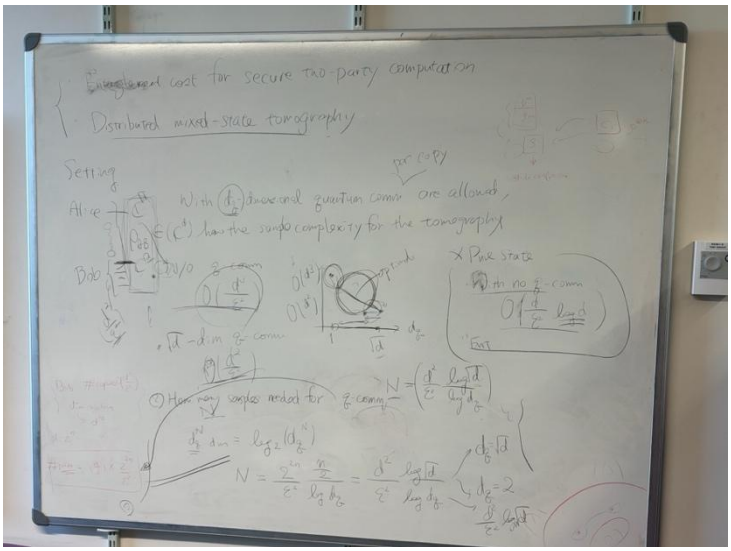
Research on distributed mixed-state tomography

The second project concerned distributed mixed-state tomography with limited quantum communication, which I discussed with Mina Doosti and Chirag Wadhwa. Quantum state tomography aims to identify an unknown state

from many copies, and in my setting the question is how this can be done when the state is distributed among multiple parties whose communication is restricted. Because this problem combines tomography with distributed quantum computation, I found it closely connected to my own background.

We began by reviewing prior work. For pure states, the optimal sample complexity and corresponding strategies are already well understood, so we decided to focus on the less understood mixed-state case. We examined several candidate approaches, including bipartite Schur basis measurement and teleportation-based methods, and identified promising directions that may achieve optimal or near-optimal sample complexity. Another interesting point was the possibility that even a small amount of quantum communication may create a gap between the achievable sample complexity and the case with no quantum communication at all. If this is true, it would show that limited quantum communication can already provide a substantial advantage in distributed mixed-state tomography. After returning to Japan, I would like to examine more carefully whether these methods are truly sample-optimal and to clarify the nature of this possible gap.

In addition, Mina introduced me to important prior papers and lecture videos on quantum tomography, which helped me quickly acquire background knowledge outside my immediate area of expertise. This was particularly valuable because it allowed me to connect tools from tomography with questions that I had previously considered mainly from the viewpoint of distributed quantum computation.



Picture 1. Discussion during the visit on distributed mixed-state tomography.

Summary

Overall, this visit was highly meaningful for my research. For the two projects, entanglement cost in secure two-party quantum computation and distributed mixed-state tomography under communication constraints, I was able to identify nontrivial and promising directions that may lead to meaningful results. After returning to Japan, I would like to investigate these ideas in greater mathematical detail. This was also my first long research visit, and it gave me many opportunities to discuss with researchers whom I had not previously known. Through these interactions, I gained a better sense of how discussions with other researchers can be incorporated into my own research. I also benefited from exchanges with researchers in quantum cryptography and tomography, fields outside my main expertise, and received valuable feedback from broader perspectives. I would like to sincerely thank Mina Doosti, Alexandru Cojocaru, Dominik Leichtle, Chirag Wadhwa, Abbas Poshtvan, and the members of the School of Informatics at the University of Edinburgh for their hospitality and valuable discussions. I am also grateful to the FoPM program for making this visit possible.

References

[1] Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail, "Secure Two-Party Quantum Evaluation of Unitaries against Specious Adversaries," in Advances in Cryptology - CRYPTO 2010, Lecture Notes in Computer Science 6223, Springer, 2010, pp. 685-706.