ISSN 2186-7437

NII Shonan Meeting Report

No. 198

New Directions in Provable Quantum Advantages

Organizers:
François Le Gall
Fang Song
Penghui Yao

December 11–15, 2023

National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-Ku, Tokyo, Japan

New Directions in Provable Quantum Advantages

Organizers:
François Le Gall, Nagoya University, Japan.
Fang Song, Portland State University, USA.
Penghui Yao, Nanjing University, China.

December 11–15, 2023

Abstract

During this *4.5-day seminar*, the *198th NII Shonan meeting* to be organized, we gathered 28 quantum computing experts from various institutions and backgrounds to discuss three specific topics. This presented an excellent opportunity to explore a variety of relevant and contemporary subjects, serving as a systematic effort to establish a stronger foundation for the field and identify new challenges ahead. In the forthcoming sections of this report, we will provide a summary of the content covered in invited talks and the three main topics discussed within the seminar's working groups.

Background and introduction

Quantum computing is emerging as a new science and technology that promises to achieve a significant scientific breakthrough. Despite several well-known quantum algorithms and protocols discovered in the past century, numerous exciting results have been found in the past decade, which have witnessed the advantages of quantum computation in various aspects.

The meeting focused on the following three topics.

1. Quantum distributed computing

   Quantum computing in the distributed setting has recently been the subject of intensive investigations. In particular, in the past few years, Le Gall and Magniez (PODC 2018), Le Gall, Rosmanis and Nishimura (STACS 2019), and Izumi and Le Gall (PODC 2019) have shown the superiority of quantum distributed algorithms over classical distributed algorithms in several major settings. The objective of this seminar was to both give an overview of this field and further investigate the computational power of quantum distributed algorithms. A first target was finding more examples in which quantum distributed algorithms can outperform classical distributed algorithms and especially developing new ones. A second goal was investigating the limitations of quantum distributed computing by clarifying the relations with the more developed area of two-party quantum communication complexity. For this purpose, the seminar invited participants with different backgrounds, in particular some experts of classical distributed algorithms interested in quantum computation and experts in quantum communication complexity interested in distributed computing.

2. Quantum games and quantum proof systems

   Games and proof systems are fundamental models in computational complexity. Quantum computation and quantum information processing provide fascinating twists with these models. In quantum complexity theory, one may consider the quantum analogs of the classical models, where the players exchange quantum messages. It has received great attention to investigate the quantum analogs of classical proof systems, including QMA (quantum analog of NP), QIP (quantum analog of IP), QMIP (quantum analog of MIP), etc. While the models inherit some similarities to their classical counterparts, they can also possess unique quantum features and lead to very different pictures of quantum complexity theory. In the classical setting, multiprover interactive proof systems are as powerful as NEXP. By a recent breakthrough result $\mathrm{MIP}^* = \mathrm{RE}$, if the provers are allowed to access quantum resources, then the systems are undecidable. Numerous novel ideas have been introduced in this line of research, which haven't been fully explored. For this sub-topic, the seminar invited experts in this area to share the progress and understanding on quantum interactive proof systems.

3. Quantum cryptography

   Quantum information processing is transforming the landscape of cryptography. A grave concern is the break of widely deployed cryptosystems due to exponential quantum speedup over best known classical algorithms

for problems such as factorization. There has been extensive effort to construct new cryptosystems in the hope of resisting attacks enabled by quantum computing, usually referred to as post-quantum cryptography, which leads to the ongoing influential standardization project at the US National Institute of Standards and Technology (NIST). This line of work has been a central target of cryptanalysis, and it is both theoretically and practically critical to investigate the possibility of faster quantum algorithms for a host of hard problems. On the other hand, when honest users are also granted the capability of quantum information processing, *quantum cryptography*, i.e., cryptographic constructions employing quantum information, has shown superiority over classical cryptography, turning impossibility into possibility. Notable examples include unconditional quantum key distribution (QKD) and composable secure computation from a trusted setup. In recent years, there has been remarkable progress on copy protection, including quantum money and software release against pirates. Thanks to the no-cloning feature of quantum information, candidates have been constructed for these tasks, which are otherwise impossible to realize classically since classical information can be replicated freely. This sub-topic aimed to advance new findings on both quantum algorithmic advantages on post-quantum cryptography and quantum cryptographic advantages in realizing copy protection and other primitives.

Aims of the meeting

The meeting concentrated on new settings and models where the capacity of quantum information processing provides provable advantages over classical means. The meeting invited leading researchers whose contributions are likely to be essential to this field and fostered discussions in-depth and stimulate brainstorming between researchers working on different topics. The meeting also strengthened the collaborations among various research communities, especially between Asian and non-Asian researchers.

Overview of Talks

Quantum supremacy

Bill Fefferman, The University of Chicago

A critical milestone on the path to useful quantum computers is quantum supremacy – a demonstration of a quantum computation that is prohibitively hard for classical computers. A leading near-term candidate, put forth by the Google/UCSB team, is sampling from the probability distributions of randomly chosen quantum circuits, which we call Random Circuit Sampling (RCS).

We study both the hardness and verification of RCS. While RCS was defined with experimental realization in mind, we show complexity theoretic evidence of hardness that is on par with the strongest theoretical proposals for supremacy. Specifically, we show that RCS satisfies an average-case hardness condition – computing output probabilities of typical quantum circuits is as hard as computing them in the worst-case, and therefore ♯P-hard. Our reduction exploits the polynomial structure in the output amplitudes of random quantum circuits, enabled by the Feynman path integral. In addition, it follows from known results that RCS satisfies an anti-concentration property, making it the first supremacy proposal with both average-case hardness and anti-concentration.

Quantum leader election

Seiichiro Tani, NTT

We give the first separation of quantum and classical pure (i.e., non-cryptographic) computing abilities with no restriction on the amount of available computing resources, by considering the exact solvability of a celebrated unsolvable problem in classical distributed computing, the "leader election problem" in anonymous networks. The goal of the leader election problem is to elect a unique leader from among distributed parties. We consider this problem for anonymous networks, in which each party has the same identifier. It is well-known that no classical algorithm can solve exactly (i.e., in bounded time without error) the leader election problem in anonymous networks, even if it is given the number of parties. This paper gives two quantum algorithms that, given the number of parties, can exactly solve the problem for any network topology in polynomial rounds and polynomial communication/time complexity with respect to the number of parties, when the parties are connected by quantum communication links. The two algorithms each have their own characteristics with respect to complexity and the property of the networks they can work on. Our first algorithm offers much lower time and communication complexity than our second one, while the second one is more general than the first one in that the second one can run even on any network, even those whose underlying graph is directed, whereas the first one works well only on those with undirected graphs. Moreover, our algorithms work well even in the case where only the upper bound of the number of parties is given. No classical algorithm can solve the problem even with zero error (i.e., without error but possibly in unbounded running time) in such cases, if the upper bound may be more than twice the number of parties. In order to keep the complexity of the second algorithm polynomially bounded, a new

classical technique is developed; the technique quadratically improves the previous bound on the number of rounds required to compute a Boolean function on anonymous networks, without increasing the communication complexity.

Quantum distributed computing updates

François Le Gall, Nagoya University

In this talk I survey recent developments in quantum distributed computing, i.e., distributed computing where the processors of the network can exchange quantum messages. After presenting recent quantum distributed algorithms for graph-theoretic problems in the CONGEST model, which are based on a distributed version of Grover search, I survey recent works investigating the potential of quantum distributed algorithms in the LOCAL model. Finally, I mention important open questions in quantum distributed computing.

Quantum one-wayness

Tomoyuki Morimae, Kyoto University

One-way functions are the minimum assumption in classical cryptography. On the other hand, in quantum cryptography where quantum computing and quantum communications are possible, recent studies suggest that one-way functions are not necessarily the minimum assumption. In this talk, I explain recently introduced several new primitives, such as pseudorandom state generators, one-way state generators, and EFI pairs, and show relations among them. I also give many open problems in this new field.

Quantum algorithms on lattice problems

Yixin Shen, King's College London

In this talk, I survey some algorithmic problems that arise from the cryptanalysis of lattice-based crytographic schemes such as the Shortest Vector problem and the Learning with Errors problem. Then I particularly focus on how quantum algorithms can help us obtain speed-ups on different approaches to solve those problems.

Quantum distributional proofs

Harumichi Nishimura, Nagoya University

The study of distributed interactive proofs was initiated by Kol, Oshman, and Saxena [PODC 2018] as a generalization of distributed decision mechanisms (proof-labeling schemes, etc.), and has received a lot of attention in recent years. In distributed interactive proofs, the nodes of an n-node network G can exchange short messages (called certificates) with a powerful prover. The goal is to decide if the input (including G itself) belongs to some language, with as few turns of interaction and as few bits exchanged between nodes and the prover as possible. There are several results showing that the size of certificates can be reduced

drastically with a constant number of interactions compared to non-interactive distributed proofs.

We introduce the quantum counterpart of distributed interactive proofs: certificates can now be quantum bits, and the nodes of the network can perform quantum computation. The first result of this paper shows that by using quantum distributed interactive proofs, the number of interactions can be significantly reduced. More precisely, our result shows that for any constant k, the class of languages that can be decided by a k-turn classical (i.e., non-quantum) distributed interactive protocol with $f(n)$-bit certificate size is contained in the class of languages that can be decided by a 5-turn distributed quantum interactive protocol with $O(f(n))$-bit certificate size. We also show that if we allow to use shared randomness, the number of turns can be reduced to 3-turn. Since no similar turn-reduction classical technique is currently known, our result gives evidence of the power of quantum computation in the setting of distributed interactive proofs as well.

As a corollary of our results, we show that there exist 5-turn/3-turn distributed quantum interactive protocols with small certificate size for problems that have been considered in prior works on distributed interactive proofs such as [Kol, Oshman, and Saxena PODC 2018, Naor, Parter, and Yogev SODA 2020].

We then utilize the framework of the distributed quantum interactive proofs to test closeness of two quantum states each of which is distributed over the entire network.

Publicly Verifiable Deletion from Minimal Assumptions

Ryo Nishimaki, NTT

We present a general compiler to add the publicly verifiable deletion property for various cryptographic primitives including public key encryption, attribute-based encryption, and quantum fully homomorphic encryption. Our compiler only uses one-way functions, or more generally hard quantum planted problems for NP, which are implied by one-way functions. It relies on minimal assumptions and enables us to add the publicly verifiable deletion property with no additional assumption for the above primitives. Previously, such a compiler needs additional assumptions such as injective trapdoor one-way functions or pseudorandom group actions [Bartusek-Khurana-Poremba, CRYPTO 2023]. Technically, we upgrade an existing compiler for privately verifiable deletion [Bartusek-Khurana, CRYPTO 2023] to achieve publicly verifiable deletion by using digital signatures.

Quantum pseudorandom scramblers

Mingnan Zhao, Nanjing University

Quantum pseudorandom state generators (PRSGs) have stimulated exciting developments in recent years. A PRSG, on a fixed initial (e.g., all-zero) state, produces an output state that is computationally indistinguishable from a Haar random state. However, pseudorandomness of the output state is not guaranteed

on other initial states. In fact, known PRSG constructions provably fail on some initial state.

We propose and construct quantum Pseudorandom State Scramblers (PRSSs), which can produce a pseudorandom state on an arbitrary initial state. In the informationtheoretical setting, we obtain a scrambler which maps an arbitrary initial state to a distribution of quantum states that is close to Haar random in total variation distance. As a result, our PRSS exhibits a dispersing property. Loosely, it can span an ϵ-net of the state space. This significantly strengthens what standard PRSGs can induce, as they may only concentrate on a small region of the state space as long as the average output state approximates a Haar random state in total variation distance.

Our PRSS construction develops a parallel extension of the famous Kac's walk, and we show that it mixes exponentially faster than the standard Kac's walk. This constitutes the core of our proof. We also describe a few applications of PRSSs. While our PRSS construction assumes a post-quantum one-way function, PRSSs are potentially a weaker primitive and can be separated from one-way functions in a relativized world similar to standard PRSGs

Communication Complexity of Private Simultaneous Quantum Messages Protocols

Akinori Kawachi, Mie University

The private simultaneous messages (PSM) model is a non-interactive version of the multiparty secure computation (MPC), which has been intensively studied to examine the communication cost of the secure computation. We consider its quantum counterpart, the private simultaneous quantum messages (PSQM) model, and examine the advantages of quantum communication and prior entanglement of this model.

In the PSQM model, k parties $P_1, ..., P_k$ initially share a common random string (or entangled states in a stronger setting), and they have private classical inputs $x_1, ..., x_k$. Every P_i generates a quantum message from the private input x_i and the shared random string (entangled states), and then sends it to the referee R. Receiving the messages from the k parties, R computes $F(x_1, ..., x_k)$ from the messages. Then, R learns nothing except for $F(x_1, ..., x_k)$ as the privacy condition.

We obtain the following results for this PSQM model. (i) We demonstrate that the privacy condition inevitably increases the communication cost in the two-party PSQM model as well as in the classical case presented by Applebaum, Holenstein, Mishra, and Shayevitz [Journal of Cryptology 33(3), 916–953 (2020)]. In particular, we prove a lower bound $(3 - o(1))n$ of the communication complexity in PSQM protocols with a shared random string for random Boolean functions of $2n$-bit input, which is larger than the trivial upper bound 2n of the communication complexity without the privacy condition. (ii) We demonstrate a factor two gap between the communication complexity of PSQM protocols with shared entangled states and with shared random strings by designing a multiparty PSQM protocol with shared entangled states for a total function that extends the two-party equality function. (iii) We demonstrate an exponential gap between the communication complexity of PSQM protocols

with shared entangled states and with shared random strings for a two-party partial function.

Advantage based on non-local games

Rahul Jain, National University of Singapore

We show a relation, based on parallel repetition of the Magic Square game, that can be solved, with probability exponentially close to 1 (worst-case input), by 1D (uniform) depth 2, geometrically-local, noisy (noise below a threshold), fan-in 4, quantum circuits. We show that the same relation cannot be solved, with an exponentially small success probability (averaged over inputs drawn uniformly), by 1D (non-uniform) geometrically-local, sub-linear depth, classical circuits consisting of fan-in 2 NAND gates. Quantum and classical circuits are allowed to use input-independent (geometrically-non-local) resource states, that is entanglement and randomness respectively. To the best of our knowledge, previous best (analogous) depth separation for a task between quantum and classical circuits was constant v/s sublogarithmic, although for general (geometrically non-local) circuits.

Our hardness result for classical circuits is based on a direct product theorem about classical communication protocols from Jain and Kundu [JK22].

As an application, we propose a protocol that can potentially demonstrate verifiable quantum advantage in the NISQ era. We also provide generalizations of our result for higher dimensional circuits as well as a wider class of Bell games.

Quantum topological data analysis

Ryu Hayakawa, Kyoto University

Topological data analysis (TDA) is an emergent field of data analysis. The critical step of TDA is computing the persistent Betti numbers. Existing classical algorithms for TDA are limited if we want to learn from high-dimensional topological features because the number of high-dimensional simplices grows exponentially in the size of the data. In the context of quantum computation, it has been previously shown that there exists an efficient quantum algorithm for estimating the Betti numbers even in high dimensions. However, the Betti numbers are less general than the persistent Betti numbers, and there have been no quantum algorithms that can estimate the persistent Betti numbers of arbitrary dimensions.

We show the first quantum algorithm that can estimate the (normalized) persistent Betti numbers of arbitrary dimensions. Our algorithm is efficient for simplicial complexes such as the Vietoris-Rips complex and demonstrates exponential speedup over the known classical algorithms.

IQP advantage

Zhengfeng Ji, Tsinghua University

Sampling problems demonstrating beyond classical computing power with noisy intermediate scale quantum (NISQ) devices have been experimentally

realized. In those realizations, however, our trust that the quantum devices faithfully solve the claimed sampling problems is usually limited to simulations of smaller-scale instances and is, therefore, indirect. The problem of verifiable quantum advantage aims to resolve this critical issue and provides us with greater confidence in a claimed advantage. Instantaneous quantum polynomial-time (IQP) sampling has been proposed to achieve beyond classical capabilities with a verifiable scheme based on quadratic-residue codes (QRC). Unfortunately, this verification scheme was recently broken by an attack proposed by Kahanamoku-Meyer.

We revive IQP-based verifiable quantum advantage by making two major contributions. Firstly, we introduce a family of IQP sampling protocols called the stabilizer scheme, which builds on results linking IQP circuits, the stabilizer formalism, coding theory, and an efficient characterization of IQP circuit correlation functions. This construction extends the scope of existing IQP-based schemes while maintaining their simplicity and verifiability. Secondly, we introduce the Hidden Structured Code (HSC) problem as a welldefined mathematical challenge that underlies the stabilizer scheme. To assess classical security, we explore a class of attacks based on secret extraction, including the KahanamokuMeyer's attack as a special case. We provide evidence of the security of the stabilizer scheme, assuming the hardness of the HSC problem. We also point out that the vulnerability observed in the original QRC scheme is primarily attributed to inappropriate parameter choices, which can be naturally rectified with proper parameter settings.

Secure key release

Shota Yamada, AIST

We introduce the notion of public key encryption with secure key leasing (PKE-SKL). Our notion supports the leasing of decryption keys so that a leased key achieves the decryption functionality but comes with the guarantee that if the quantum decryption key returned by a user passes a validity test, then the user has lost the ability to decrypt. Our notion is similar in spirit to the notion of secure software leasing (SSL) introduced by Ananth and La Placa (Eurocrypt 2021) but captures significantly more general adversarial strategies.

Our results can be summarized as follows:

1. **Definitions:** We introduce the definition of PKE with secure key leasing and formalize a security notion that we call indistinguishability against key leasing attacks (IND-KLA security). We also define a one-wayness notion for PKE-SKL that we call OW-KLA security and show that an OW-KLA secure PKE-SKL scheme can be lifted to an IND-KLA secure one by using the (quantum) Goldreich-Levin lemma.

2. **Constructing IND-KLA PKE with Secure Key Leasing:** We provide a construction of OW-KLA secure PKE-SKL (which implies IND-KLA secure PKE-SKL as discussed above) by leveraging a PKE scheme that satisfies a new security notion that we call consistent or inconsistent security against key leasing attacks (CoIC-KLA security). We then construct a CoIC-KLA secure PKE scheme using 1-key Ciphertext-Policy

Functional Encryption (CPFE) that in turn can be based on any IND-CPA secure PKE scheme.

3. **Identity Based Encryption, Attribute Based Encryption and Functional Encryption with Secure Key Leasing:** We provide definitions of secure key leasing in the context of advanced encryption schemes such as identity based encryption (IBE), attribute-based encryption (ABE) and functional encryption (FE). Then we provide constructions by combining the above PKE-SKL with standard IBE, ABE and FE schemes.

Notably, our definitions allow the adversary to request distinguishing keys in the security game, namely, keys that distinguish the challenge bit by simply decrypting the challenge ciphertext, as long as it returns them (and they pass the validity test) before it sees the challenge ciphertext. All our constructions satisfy this stronger definition, albeit with the restriction that only a bounded number of such keys is allowed to the adversary in the IBE and ABE (but not FE) security games.

Prior to our work, the notion of single decryptor encryption (SDE) has been studied in the context of PKE (Georgiou and Zhandry, Eprint 2020) and FE (Kitigawa and Nishimaki, Asiacrypt 2022) but all their constructions rely on strong assumptions including indistinguishability obfuscation. In contrast, our constructions do not require any additional assumptions, showing that PKE/IBE/ABE/FE can be upgraded to support secure key leasing for free.

From the Hardness of Detecting Superpositions to Cryptography

Minki Hhan, KIAS

Recently, Aaronson et al. (arXiv:2009.07450) showed that detecting interference between two orthogonal states is as hard as swapping these states. While their original motivation was from quantum gravity, we show its applications in quantum cryptography.

1. We construct the first public key encryption scheme from cryptographic non-abelian group actions. Interestingly, the ciphertexts of our scheme are quantum even if messages are classical. This resolves an open question posed by Ji et al. (TCC '19). We construct the scheme through a new abstraction called swap-trapdoor function pairs, which may be of independent interest.

2. We give a simple and efficient compiler that converts the flavor of quantum bit commitments. More precisely, for any prefix $X, Y \in \{$computationally, statistically, perfectly$\}$, if the base scheme is X-hiding and Y-binding, then the resulting scheme is Y-hiding and X-binding. Our compiler calls the base scheme only once. Previously, all known compilers call the base schemes polynomially many times (Crépeau et al., Eurocrypt'01 and Yan, Asiacrypt'22). For the security proof of the conversion, we generalize the result of Aaronson et al. by considering quantum auxiliary inputs.

Unstructured quantum advantage

Takashi Yamakawa, NTT

We show the following hold, unconditionally unless otherwise stated, relative to a random oracle with probability 1:

- There are NP search problems solvable by BQP machines but not BPP machines.
- There exist functions that are one-way, and even collision resistant, against classical adversaries but are easily inverted quantumly. Similar separations hold for digital signatures and CPA-secure public key encryption (the latter requiring the assumption of a classically CPA-secure encryption scheme). Interestingly, the separation does not necessarily extend to the case of other cryptographic objects such as PRGs.
- There are unconditional publicly verifiable proofs of quantumness with the minimal rounds of interaction: for uniform adversaries, the proofs are non-interactive, whereas for nonuniform adversaries the proofs are two message public coin.
- Our results do not appear to contradict the Aaronson-Ambanis conjecture. Assuming this conjecture, there exist publicly verifiable certifiable randomness, again with the minimal rounds of interaction.

By replacing the random oracle with a concrete cryptographic hash function such as SHA2, we obtain plausible Minicrypt instantiations of the above results. Previous analogous results all required substantial structure, either in terms of highly structured oracles and/or algebraic assumptions in Cryptomania and beyond.

Recursive QAOA

Eunok Bae, KIAS

Quantum approximate optimization algorithms are hybrid quantum-classical variational algorithms designed to approximately solve combinatorial optimization problems such as the MAXCUT problem. In spite of its potential for near-term quantum applications, it has been known that quantum approximate optimization algorithms have limitations for certain instances to solve the MAX-CUT problem, at any constant level p. Recently, the recursive quantum approximate optimization algorithm, which is a non-local version of quantum approximate optimization algorithm, has been proposed to overcome these limitations. However, it has been shown by mostly numerical evidences that the recursive quantum approximate optimization algorithm outperforms the original quantum approximate optimization algorithm for specific instances. We analytically prove that the recursive quantum approximate optimization algorithm is more competitive than the original one to solve the MAX-CUT problem for complete graphs with respect to the approximation ratio.

List of Participants

- Eunok Bae, KIAS
- Kai-Min Chung, Academia Sinica
- Bill Fefferman, The University of Chicago
- Honghao Fu, MIT
- Ryu Hayakawa, Kyoto University
- Taisuke Izumi, Osaka University
- Rahul Jain, National University of Singapore
- Zhengfeng Ji, Tsinghua University
- Akinori Kawachi, Mie University
- Minki Khan, KIAS
- François Le Gall (Organizer), Nagoya University
- Yinan Li, Wuhan University
- Han-Hsuan Lin, National Tsing Hua University
- Tomoyuki Morimae, Kyoto University
- Iu-iong Ng, Nagoya University
- Ryo Nishimaki, NTT
- Harumichi Nishimura, Nagoya University
- Yixin Shen, King's College London
- Fang Song (Organizer), Portland State University
- Suguru Tamaki, University of Hyogo
- Seiichiro Tani, NTT
- Chunhao Wang, Pennsylvania State University
- Pei Wu, Weizmann Institute of Science
- Shota Yamada, AIST
- Takashi Yamakawa, NTT
- Penghui Yao (Organizer), Nanjing University
- Mingnan Zhao, Nanjing University

Meeting Schedule

The seminar is a five-day event focused on three topics of quantum computing. Each day follows a structured format with a balance of informative talks, interactive discussions, networking opportunities, and social events, ensuring attendees have a fulfilling and enriching experience throughout the meeting.

Check-in Day: December 10 (Sun)

- 15:00 – 19:00 Check-in
- 19:00 – 21:00 Welcome Banquet

Day 1: December 11 (Mon)

- 7:30 – 9:00 Breakfast
- 9:00 – 9:15 Opening Remarks
- 9:15 – 10:00 Bill Fefferman: *Quantum supremacy*
- 10:00 – 10:30 Discussion
- 10:30 – 11:00 Coffee Break
- 11:00 – 11:30 Seiichiro Tani: *Quantum leader election*
- 11:30 – 12:00 François Le Gall: *Quantum distributed computing updates*
- 12:00 – 13:30 Lunch
- 13:30 – 14:00 Group Photo
- 14:00 – 14:45 Tomoyuki Morimae: *Quantum one-wayness*
- 14:45 – 15:00 Discussion: *Quantum cryptographic advantages*
- 15:00 – 15:30 Coffee Break
- 15:30 – 17:00 Breakout groups: open problems
- 18:00 – 19:30 Dinner

Day 2: December 12 (Tue)

- 7:30 – 9:00 Breakfast
- 9:00 – 9:45 Yixin Shen: *Quantum algorithms on lattice problems*
- 10:00 – 10:30 Harumichi Nishimura: *Quantum distributional proofs*
- 10:30 – 11:00 Coffee Break
- 11:00 – 11:45 Breakout groups
- 12:00 – 13:30 Lunch

- 14:00 – 14:30 Ryo Nishimaki: *Publicly Verifiable Deletion from Minimal Assumptions*
- 14:30 – 15:00 Mingnan Zhao: *Quantum pseudorandom scramblers*
- 15:00 – 15:30 Coffee Break
- 15:30 – 17:00 Breakout groups
- 18:00 – 19:30 Dinner
- 19:30 – 21:00 Research party @ Research Wing Lounge

Day 3: December 13 (Wed)

- 7:30 – 9:00 Breakfast
- 9:00 – 9:45 Akinori Kawachi: *Communication Complexity of Private Simultaneous Quantum Messages Protocols*
- 10:00 – 10:30 Rahul Jain: *Advantage based on non-local games*
- 10:30 – 11:00 Coffee Break
- 11:00 – 11:45 Breakout groups
- 12:00 – 13:30 Lunch
- 13:30 – 18:00 Excursion
- 18:15 – 21:00 Main Banquet

Day 4: December 14 (Thu)

- 7:30 – 9:00 Breakfast
- 9:00 – 9:45 Ryu Hayakawa: *Quantum topological data analysis*
- 10:00 – 10:30 Zhengfeng Ji: *IQP advantage*
- 10:30 – 11:00 Coffee Break
- 11:00 – 11:45 Breakout groups
- 12:00 – 13:30 Lunch
- 14:00 – 14:30 Shota Yamada: *Secure key release*
- 14:45 – 15:30 Minki Hhan: *From the Hardness of Detecting Superpositions to Cryptography*
- 15:30 – 16:00 Coffee Break
- 16:00 – 17:30 Open discussion
- 18:00 – 19:30 Dinner
- 19:30 – 21:00 Research party @ Research Wing Lounge

Day 5: December 15 (Fri)

- 7:30 – 9:00 Breakfast
- 9:00 – 9:45 Takashi Yamakawa: *Unstructured quantum advantage*
- 10:00 – 10:30 Eunok Bae: *Recursive QAOA*
- 10:30 – 11:00 Coffee Break
- 11:00 – 11:45 Breakout groups
- 12:00 – 13:30 Lunch
- 13:30 Farewell

Summary and future directions

Quantum supremacy on NISQ devices One of the key themes of this meeting is quantum supremacy on NISQ devices. Several approaches were proposed to achieve quantum supremacy in the past decade, most of which are sampling-based problems. Two presentations at this meeting delve into quantum sampling problems and quantum supremacy.

In one of the talk by Bill Fefferman, the focus was on the theoretical challenges surrounding the quantum supremacy of Random Circuit Sampling (RCS), an algorithm that has been implemented by several experimental groups. Howevever, there are still several unsolved problems regarding RCS. Fefferman's presentation addressed various aspects of the computational complexity associated with RCS and the technical challenges involved in its verification. The other talk by Zhengfeng discussed Instantaneous Quantum Polynomial-Time (IQP) sampling, considered one of the earliest sampling problems believed to be classically hard. The initial IQP sampling protocol was thought to be verifiable, but this belief was later falsified. Ji put forward a new verifiable IQP-based quantum advantage leveraging certain complexity-theoretical assumption. These two talks spur the discussion of verifiable quantum advantages of NISQ devices.

Quantum Cryptographic Advantages. Heated discussions arose following the talks on novel quantum cryptographic primitives and the possibility of basing quantum cryptography on weaker assumptions that what researchers believed necessary before. In particular, Morimae's talk depicted a state-of-art landscape of quantum cryptography, dubbed *microcrypt*. (See a summary in Figure 2 below).

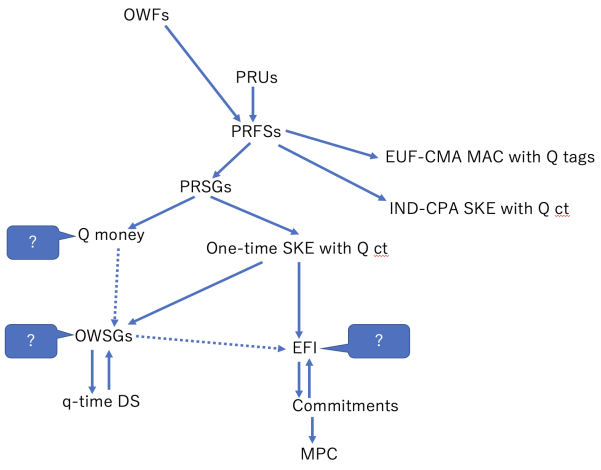

Figure 2: New primitives and assumptions in quantum cryptography.

A number of open questions were proposed in the talk, and attempts to tackle those emerge frequently in the following discussions, which also generated new questions that broaden the horizon (and sometimes making the reality all the more puzzling). A few examples include:

- Can the output length of a pseudorandom state generator be adjusted

flexibly? This is a useful feature that is easily achievable by a classical pseudorandom string generator.

- What is the full capability of one-way state generators (OWSGs)? Is it possible to base quantum money on OWSGs?
- Given the diverse but also convoluted primitives at the moment, is there a fundamental primitive that unifies all, à la one-way functions in classical cryptography?

Advantages of quantum distributed computing. The talks on quantum distributed computing held on the first day of the workshop gave a comprehensive overview of quantum algorithms for leader election and recent updates in quantum distributed algorithms. They were followed by many discussions during the workshop. Several discussions focused on finding new examples that exhibit a quantum advantage over classical distributed algorithms. The main target was identified as Locally Checkable Problems (LCPs) in the LOCAL model, such as graph coloring and similar locally checkable graph-theoretic problems. These problems, which have a relatively simple structure and are thus good targets for proving lower bounds, are at the center of recent developments in classical distributed computing. Discussions between experts in quantum distributed algorithms and experts in quantum cryptography also lead to the following proposal: show the quantum (exponential) advantage in the distributed setting under "weak" security requirements, i.e., security requirements weaker than those typically used in multiparty secure computation.

Classical and quantum communication complexity Communication complexity serves as a versatile tool for establishing lower bounds on the advantages and complexity of quantum distributed computing. Much of the prior research in this area is concentrated on the model of two-party interactive communication. However, the study of quantum distributed computing has spurred interest in the study of multiparty quantum communication complexity on networks possessing more complicated topologies.

Although there have not been many talks directly addressing quantum communication complexity, workshops have indeed sparked considerable discussion on this topic, including classical and quantum multiparty communication complexity. After François Le Gall's survey talk on quantum distributed computing, One of the most relevant problems in quantum communication complexity has been raised and discussed in depth in the workshop, which is proving a tight bound on the multiparty quantum communication complexity of SET-DISJOINTNESS in the number-in-hand model. Akinori Kawachi's talk provided an overview of the communication complexity of secure computation, an area that remains largely unexplored. In particular, there exists an exponential separation between the most efficient known protocols and the best lower bound for most of the problems. Rahul Jain's talk prompts the discourse on the applications of communication complexity in proving the advantages of quantum circuits for generating certain correlations. The primary techniques involved reducing the difficulty to proving the classical communication complexity of correlation generation. An interesting follow-up question is whether any more provable quantum advantages can be obtained via communication complexity.

Conclusion

During our 4.5-day seminar, we brought together 28 quantum computing experts from a range of institutions, backgrounds, and specializations to delve into the specifics of our field. The focus of the meeting was exploring new scenarios and models where quantum information processing clearly outperforms classical methods. This gathering offered a valuable opportunity to delve into various relevant and contemporary topics, laying the groundwork for our field, and anticipating forthcoming challenges. By inviting key researchers whose contributions are indispensable to the field, the seminar sparked in-depth discussions and brainstorming sessions between experts working on diverse topics. Furthermore, the meeting facilitated enhanced collaborations among different research communities, with a notable focus on strengthening ties between Asian and non-Asian researchers.

A research paper generated from this meeting. We were made aware when preparing this report that three participants of this shonan meeting, Minki Hhan, successfully resolved an open question discussed during the meeting with continued effort. The authors acknowledged Shonan meeting for this accomplishment.

> A Note on Output Length of One-Way State Generators.
>
> Minki Hhan, Tomoyuki Morimae, Takashi Yamakawa.
>
> ArXiv preprint arXiv:2312.16025, 2023