External Awards

Volunteer Service Award

Winner: Daisuke Ikegami, NTT Network Technology Laboratories
Date: September 11, 2019
Organization: The Institute of Electronics, Information and Communication Engineers (IEICE) Technical Committee on Communication Quality (CQ)

For his contribution to the CQ committee as an expert member.

Specially Selected Paper

Winner: Yuta Sawabe, Waseda University; Daiki Chiba and Mitsuaki Akiyama, NTT Secure Platform Laboratories; Shigeki Goto, Waseda University
Date: September 15, 2019
Organization: Information Processing Society of Japan

For "Detection Method of Homograph Internationalized Domain Names with OCR."

Published as: Y. Sawabe, D. Chiba, M. Akiyama, and S. Goto, "Detection Method of Homograph Internationalized Domain Names with OCR," J. Info. Process, Vol. 27, pp. 536–544, Sept. 2019.

Papers Published in Technical Journals and Conference Proceedings

Random Quantum Circuit Sampling with Global Depolarizing Noises

T. Morimae, Y. Takeuchi, and S. Tani

arXiv:1911.02220 [quant-ph], November 2019.

A recent paper [F. Arute et al. Nature 574, 505 (2019)] considered exact classical sampling of the output probability distribution of the globally depolarized random quantum circuit. In this paper, we discuss three results. First, we consider the case in which the fidelity F is constant. We show that if the distribution is classically sampled in polynomial time within a constant multiplicative error, then BQP $\subseteq$ SBP, which means that BQP is in the second level of the polynomial-time hierarchy. We next show that for any $F \leq 1/2$, the distribution is classically trivially sampled by the uniform distribution within the multiplicative error $F2^{n+2}$, where n is the number of qubits. We finally show that for any F, the distribution is classically trivially sampled by the uniform distribution within the additive error $2F$. These last two results indicate that if we consider realistic cases, both $F \sim 2^{-m}$ and $m \gg n$, or at least $F \sim 2^{-m}$, where m is the number of gates, quantum supremacy does not exist for approximate sampling even with exponentially small errors. We also argue that if $F \sim 2^{-m}$ and $m \gg n$, the standard approach will not work to show quantum supremacy even for exact sampling.

Sumcheck-based Delegation of Quantum Computing to Rational Server

Y. Takeuchi, T. Morimae, and S. Tani

arXiv:1911.04734 [quant-ph], November 2019.

Delegated quantum computing enables a client with weak computational power to delegate quantum computing to a remote quantum server in such a way that the integrity of the server is efficiently verified by the client. A new model of delegated quantum computing has recently been proposed, namely, rational delegated quantum computing. In this model, after the client interacts with the server, the client pays a reward to the server depending on the server's messages and client's random bits. The rational server sends messages that maximize the expected value of the reward. It is known that the classical client can delegate universal quantum computing to the rational quantum server in one round. In this paper, we propose one-round rational delegated quantum computing protocols by generalizing the classical rational sumcheck protocol. An advantage of our protocols is that they are gate-set independent: the construction of the previous rational protocols depends on gate sets, while our sumcheck-based protocols can be easily realized any local gate set (the elementary gates of each can be specified with a polynomial number of bits). As with the previous protocols, our reward function satisfies natural requirements (non-negative, upper-bounded by a constant, and its maximum expected value is lower-bounded by a constant). We also discuss the reward gap. Simply speaking, the reward gap is a minimum loss on the expected value of the server's reward incurred by the server's behavior that makes the client accept an incorrect answer. The reward gap therefore should be large enough to incentivize the server to behave optimally. Although our sumcheck-based protocols have only exponentially small reward gaps, as with the previous protocols, we show that a constant reward gap can be achieved if two non-communicating but entangled rational servers are allowed. We also discuss that a single rational server is sufficient under the (widely believed) assumption that the learning-with-errors problem is hard for polynomial-time quantum computing. Apart from these results, we show, under a certain condition, the equivalence between rational and ordinary delegated quantum computing protocols. Based on this equivalence, we give a reward-gap amplification method.