External Awards

IPSJ Fellow

Winner: Makoto Iwamura, NTT Social Informatics Laboratories/NTT Security (Japan) KK
Date: March 28, 2022
Organization: Information Processing Society of Japan (IPSJ)

For his contribution to the development of pioneering anti-cyber-attack technologies and revitalization of the security field through industry-academia cooperation.

Specially Selected Paper

Winners: Yukako Iimura, NTT Computer and Data Science Laboratories; Shinobu Saito, NTT Computer and Data Science Laboratories
Date: April 18, 2022
Organization: IPSJ

For "Industrial Practice and Evaluation of Microtask Programming for Achieving Working Style Diversity."
Published as: Y. Iimura and S. Saito, "Industrial Practice and Evaluation of Microtask Programming for Achieving Working Style Diversity," IPSJ Journal, Vol. 63, No. 4, pp. 999–1007, Apr. 2022.

Best Paper Award

Winners: Takafumi Tanaka, NTT Network Innovation Laboratories; Seiki Kuwabara, NTT Network Innovation Laboratories/NTT Communications; Tetsuro Inui, NTT Network Innovation Laboratories
Date: May 11, 2022
Organization: The Institute of Electronics, Information and Communication Engineers (IEICE) Communications Society

For "Demonstration of Flex Ethernet over OTN Link State Monitoring Method."
Published as: T. Tanaka, S. Kuwabara, and T. Inui, "Demonstration of Flex Ethernet over OTN Link State Monitoring Method," IEICE Trans. Commun. (JPN Edition), Vol. J103-B, No. 11, pp. 595–604, Nov. 2020.

Kenneth C. Smith Early Career Award in Microelectronics

Winner: Akira Ito, NTT Social Informatics Laboratories
Date: May 21, 2022
Organization: The Institute of Electrical and Electronics Engineers (IEEE) Computer Society, Technical Community on Multiple-Valued Logic

For "A Formal Approach to Identifying Hardware Trojans in Cryptographic Hardware."
Published as: A. Ito, R. Ueno, and N. Homma, "A Formal Approach to Identifying Hardware Trojans in Cryptographic Hardware," 2021 IEEE 51st International Symposium on Multiple-Valued Logic (ISMVL), pp. 154–159, Nur-Sultan, Kazakhstan, May 2021.

Standardization Achievement Award

Winner: Seishi Takamura, NTT Computer and Data Science Laboratories
Date: May 24, 2022
Organization: IPSJ/Information Technology Standards Commission of Japan

For his long-term contribution to the standardization activities in International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Joint Technical Committee 1 Subcommittee 29 since 1998.

IPSJ Fellow

Winner: Seishi Takamura, NTT Computer and Data Science Laboratories
Date: June 7, 2022
Organization: IPSJ

For his achievement concerning the research and development of video coding and contribution to its standardization and dissemination.

IACR Fellow

Winner: Masayuki Abe, NTT Social Informatics Laboratories
Date: June 27, 2022
Organization: The International Association for Cryptologic Research (IACR)

For influential contributions to practical cryptosystems and for exemplary service to the IACR and the Asia-Pacific cryptography community.

Papers Published in Technical Journals and Conference Proceedings

Sumcheck-based Delegation of Quantum Computing to Rational Server

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

Theoretical Computer Science, Vol. 924, No. 1, pp. 46–67, April 2022.

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 can be efficiently verified by the client. Recently, a new model of delegated quantum computing has 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 the 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 novel 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 technique can be easily realized with any local gate set (each of whose elementary gates can be specified with a polynomial number of bits). Furthermore, as with the previous protocols, our reward function satisfies natural requirements (the reward is 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 should therefore be large enough to incentivize the server to behave optimally. Although our sumcheck-based protocols have only exponentially small reward gaps as in the previous protocols, we show that a constant reward gap can be achieved if two noncommunicating but entangled rational servers are allowed. We also discuss whether 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. This equivalence then serves as a basis for a reward-gap amplification method.

Rewindable Quantum Computation and Its Equivalence to Cloning and Adaptive Postselection

R. Hiromasa, A. Mizutani, Y. Takeuchi, and S. Tani

arXiv:2206.05434, June 2022.

We define rewinding operators that invert quantum measurements. Then, we define complexity classes RwBQP, CBQP, and AdPostBQP as sets of decision problems solvable by polynomial-size quantum circuits with a polynomial number of rewinding operators, cloning operators, and (adaptive) postselections, respectively. Our main result is that $\mathrm{BPP}^{\mathrm{PP}} \subseteq \mathrm{RwBQP} = \mathrm{CBQP} = \mathrm{AdPostBQP} \subseteq \mathrm{PSPACE}$. As a byproduct of this result, we show that any problem in PostBQP can be solved with only postselections of outputs whose probabilities are at least some constant. Under the strongly believed assumption that the shortest independent vectors problem cannot be efficiently solved with quantum computers, we also show that a single rewinding operator is sufficient to achieve a task that is intractable for quantum computation. In addition, we consider rewindable Clifford and instantaneous quantum polynomial time circuits.
