IEEE Transactions on Quantum Engineering

Received 4 July 2023; accepted 11 July 2023; date of publication 18 July 2023;
date of current version 4 August 2023.

Digital Object Identifier 10.1109/TQE.2023.3296458

Corrections to "The Present and Future of Discrete Logarithm Problems on Noisy Quantum Computers"

YOSHINORI AONO[1,5], SITONG LIU[2], TOMOKI TANAKA[3], SHUMPEI UNO[4], RODNEY VAN METER[5,6] (Senior Member, IEEE), NAOYUKI SHINOHARA[1], AND RYO NOJIMA[1,7]

[1]National Institute of Information and Communications Technology, Tokyo 184-8795, Japan
[2]Graduate School of Media and Governance, Keio University, Kanagawa 252-0882, Japan
[3]Mitsubishi UFJ Financial Group, Inc. and MUFG Bank, Ltd., Tokyo 100-8388, Japan
[4]Mizuho Research & Technologies, Ltd., Tokyo 101-8443, Japan
[5]Quantum Computing Center, Keio University, Kanagawa 223-8522, Japan
[6]Faculty of Environment and Information Studies, Keio University, Kanagawa 252-0882, Japan
[7]College of Information Science and Engineering, Ritsumeikan University, Shiga 525-8577, Japan

Corresponding author: Yoshinori Aono (e-mail: aono@nict.go.jp).

In our article [1], the authors have found incorrect implementations of a postprocessing algorithm (Algorithm 1) as a result of which it is necessary to modify Figs. 8–10.

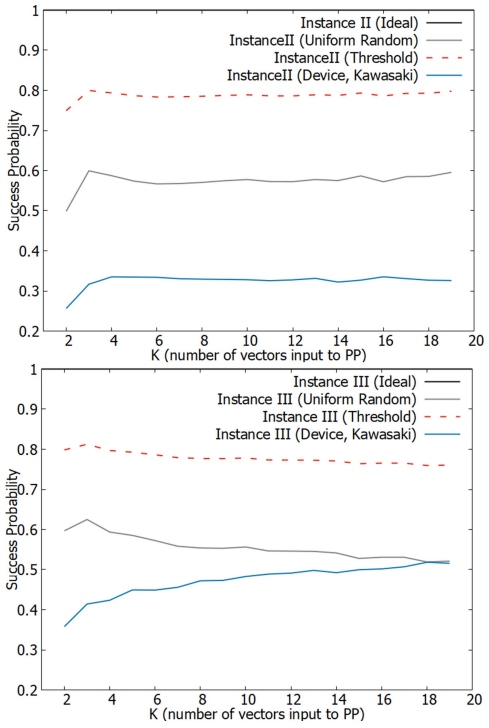

FIGURE 1. Corrections to Fig. 8. The conclusion that the output of Kawasaki device without modification do not reach the threshold success probability remains unchanged.

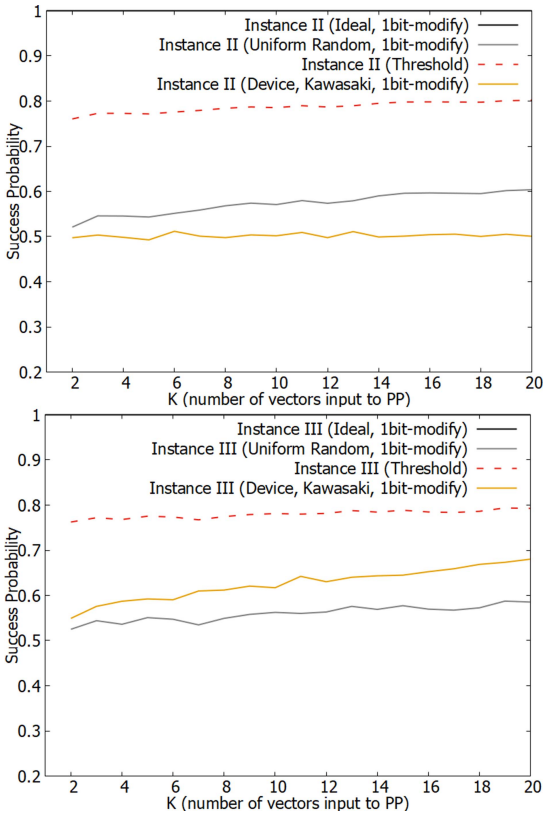

FIGURE 2. Corrections to Fig. 9. The conclusion that the output of Kawasaki device with modification do not reach the threshold success probability remains unchanged.

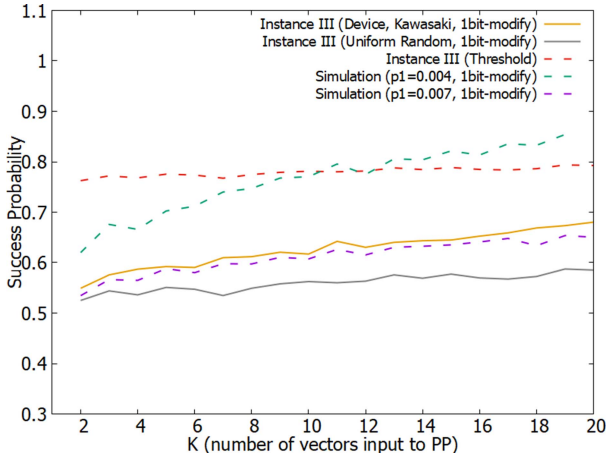

FIGURE 3. **Corrections to Fig. 10. The conclusions of the experiments remain unchanged. The output of Kawasaki device follows the simulation noise level 0.07 and do not reach the threshold success probability, also, the simulation noise level 0.04 can reach the threshold.**

In Step 5 of the algorithm, the CVP subroutine sometimes returns multiple vectors whose distances are all equivalent. To select a candidate, we represent the vectors by linear combinations of lattice basis vectors and then we took the first vector after the sort by its combination coefficients. This deterministic selection resulted in biases in the small K cases in the published article. To eliminate this bias, we modified the postprocessing algorithm to select a random vector from the set as a candidate, then reexecuted the same computer experiments reported in the article. Fig. 8 from the article is redrawn as Fig. 1 here using the corrected data, Fig. 9 is redrawn as Fig. 2, and Fig. 10 is redrawn as Fig. 3. The overall conclusion on the future of discrete logarithm problems is not changed.

REFERENCE

[1] Y. Aono et al., "The present and future of discrete logarithm problems on noisy quantum computers," *IEEE Trans. Quantum Eng.*, vol. 3, 2022, Art. no. 3102021, doi: 10.1109/TQE.2022.3183385.