Abstract Submitted
for the DAMOP18 Meeting of
The American Physical Society

Exponential quantum randomness expansion with trapped ions based on contextuality[1] MARK UM, QI ZHAO, JUNHUA ZHANG, PENGFEI WANG, YE WANG, MU QIAO, HONGYI ZHOU, IIIS, Tsinghua University, KAI-MIN CHUNG, IIS, Taiwan, XIONGFENG MA, KIHWAN KIM, IIIS, Tsinghua University — We report a self-testing quantum random number generator (QRNG) achieving an exponential gain of randomness expansion. Similar to Bell's theorem [1], violation of Kochen and Specker theory, which also presents the intrinsic randomness of quantum mechanics and excludes noncontextual hidden variable models, is also used to certify generated randomness [2]. Here, we employ an extended Klyachko-Can-Binicoglu-Shumovsky (KCBS) inquality [4,5] on a qutrit system of a trapped 138Ba+ ion system. Furthermore, by applying a spot-checking protocol of [3], our self-testing QRNG realizes exponential randomness expansion without independent and identically distributed assumption considering the most general quantum adversary scenario. The system demonstrates 1.2410ˆ8 trials and results in randomness extraction of 2.310ˆ5 bits realizing a 6.610ˆ4 bits exponential randomness expansion with the speed of 270 bits/s. [1] S. Pironio, et al., Nature 464, 1021 (2010). [2] Mark Um, et al., Sci. Rep. 3, 1627 (2013). [3] Carl Miller and Yaoyun Shi, Siam J. Comput. 46, 1304 (2017). [4] O. Guhne, et al., Phys. Rev. A 81, 022121 (2010). [5] J. Szangolies, et al., Phys. Rev. A. 87, 050101 (2013).

[1]This work was supported by the National Basic Research Program of China Grant 11CBA00300, 2011CBA00301, the National Natural Science Foundation of China Grant 11374178 and 11574002.

Mark Um
IIIS, Tsinghua University

Date submitted: 08 May 2018 Electronic form version 1.4