SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

LWE 問題を用いたマジック状態生成機能の検証
Computational self-testing for entangled magic states

竹内 勇貴 * 水谷 明博 † 廣政 良 † 相川 勇輔 † 谷 誠一郎 *
Yuki Takeuchi Akihiro Mizutani Ryo Hiromasa Yusuke Aikawa Seiichiro Tani

キーワード LWE 問題, 量子計算, セルフテスト, マジック状態

あらまし

量子計算機が指定された状態生成と測定を正しく行なっているかを検証するプロトコルはセルフテスト [1] と呼ばれている．セルフテストは紛失通信 (Oblivious transfer) [2] や量子暗号 [3] に応用可能であり，暗号プロトコルの構成要素としても重要な概念である．従来のセルフテストでは，複数の量子計算機を準備し，それらが互いに通信を行なっていないことを仮定する必要があった (図 1)．近年，ベル状態と呼ばれる一部の量子状態に対して，LWE 問題 [4] の困難性を利用することでこの仮定を取り除く方法が提案された [5]．しかし，ベル状態は量子計算機で効率良くシミュレート可能な状態であるため，彼らの結果を量子計算に応用することは困難である．そこで，我々は，同様の結果を，量子計算機実現において重要な量子状態である，CCZ ゲートに対するマジック状態に拡張した [6]．また，既存の方法では，T ゲートに対するマジック状態のセルフテストは構成出来ないことも示した．

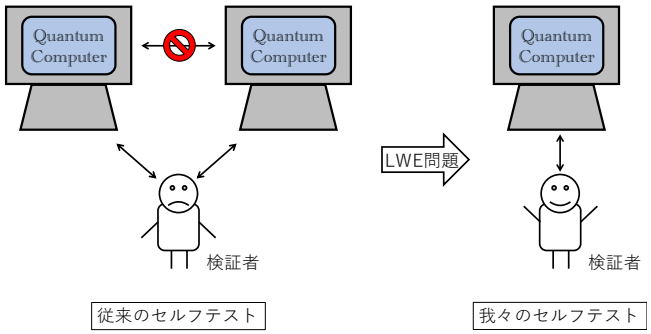

図 1: 従来のセルフテストでは，複数の量子計算機を準備し，それらが互いに通信しないことを保障しなければならないという欠点があった．文献 [5] や我々の結果では，LWE 問題の困難性を利用して，必要な量子計算機を 1 つにすることで，この欠点を解決できる．

参考文献

[1] D. Mayers and A. Yao, “Self testing quantum apparatus,” Quantum Inf. Comput. **4**, 273 (2004).

[2] A. Broadbent and P. Yuen,“Device-Independent Oblivious Transfer from the Bounded-Quantum-Storage-Model and Computational Assumptions,” arXiv:2111.08595 (2021).

[3] T. Metger, Y. Dulek, A. W. Coladangelo, and R. Arnon-Friedman, “Device-independent quantum key distribution from computational assumptions,” New J. Phys. (2021).

[4] O. Regev, “On lattices, learning with errors, random linear codes, and cryptography,” in *Proc. of the 37th Annual Symposium on Theory of Computing* (ACM, New York, 2005), p. 84.

[5] T. Metger and T. Vidick, “Self-testing of a single quantum device under computational assumptions,” Quantum **5**, 544 (2021).

[6] A. Mizutani, Y. Takeuchi, R. Hiromasa, Y. Aikawa, and S. Tani, “Computational self-testing for entangled magic states,” Cryptology ePrint Archive: Report 2021/1473 (2021).

* 日本電信電話株式会社 コミュニケーション科学基礎研究所, 〒 243-0198 神奈川県厚木市森の里若宮 3-1, NTT Communication Science Laboratories, NTT Corporation, Atsugi, Kanagawa 243-0198
† 三菱電機株式会社 情報技術総合研究所, 〒 247-8501 神奈川県鎌倉市大船 5-1-1, Mitsubishi Electric Corporation, Information Technology R&D Center, Kamakura, Kanagawa 247-8501