Entanglement Quantum Random Number Generator with public randomness certification

J. Jacak, W. Jacak, W. Donderowicz, L. Jacak
Department of Quantum Technologies, Wrocław University of Science and Technology
Wybrzeże Wyspiańskiego 27, 50-370, Wrocław, Poland
CompSecur sp. z o.o. ul. Piłsudskiego 74, 52-020, Wrocław, Poland

As Quantum Random Number Generators are gaining in popularity, especially in regard to still considered possibility of construction of a scalable, universal quantum computer in the near future, an original new protocol is proposed in randomness generation based on properties of the topologically inequivalent types of multi-qubit quantum entanglement. The newly described Entanglement Quantum Random Number Generator (Entanglement QRNG) protocol uses a certain type of multi-qubit entanglement of quantum states to produce randomness with previously non-achievable result of the feasibility of public testing for randomness certification without unveiling of the generated random bits, which remain secret (in an information-theoretic sense, what results from secrecy and quantum randomness of the correlation types).

The paper describes both the protocol and its generic implementation in quantum circuits (cf. figure below) with in depth analysis and discussion of the protocol properties, involving the specific 3-qubits quantum entanglement of generalized Bell state type, topologically inequivalent to other possible different type of maximal level 3-qubits entanglement and easily generalized to multiple-qubits as explained in the paper. The result is characterized in the formalism of quantum information as well as in topological terms. The proposed EQRNG protocol offers for the first time a secret random number generation based on a non-deterministic quantum process with a property of publicly accessible testing for randomness verification and certification without unveiling its secrecy. This property corresponds to some extent to the concept of the device independent randomness generation, but in a completely new way it offers public verification of the randomness, thus enabling an external party to freely and publicly verify the randomness of the quantum generated sequence – without disclosing of its secrecy or distorting it in any way (which is of a critical importance for any prospective practical QRNG application in both quantum and classical cryptography).

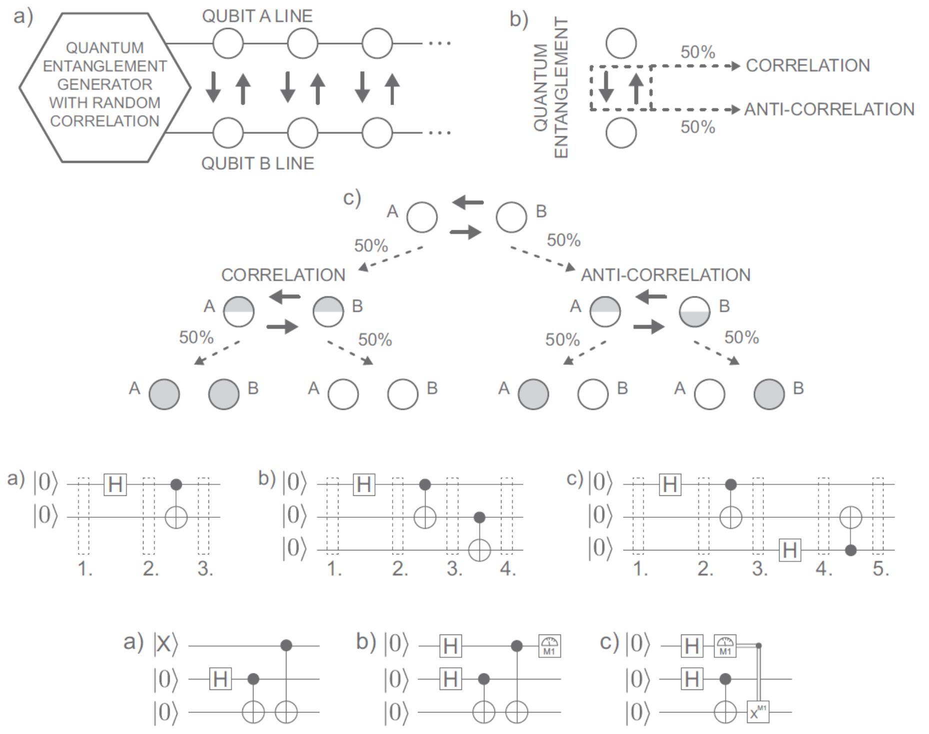

Fig. 1. Principle of the proposed EQRNG protocol operation along with its quantum circuits implementation based on the two possible correlation types randomly projected in measurement