Article

Quantum random number generator protocols based on topologically inequivalent entanglements of quantum states

Witold A. Jacak †, **Janusz E. Jacak** †, **Wojciech A. Donderowicz** † **and Lucjan Jacak** †

† These authors contributed equally to this work.

November 1, 2017 submitted to Entropy

Abstract: As the quantum random number generators are gaining in popularity, especially with regard to possibility of construction of a scalable quantum computer, some new theoretical perspectives in this research area, especially involving topological properties of quantum entanglement seem to be of interest. Application of the topologically inequivalent entanglements of quantum states for fundamental quantum information protocols like quantum teleportation or quantum random numbers generators is discussed. We present a simple protocol, involving specific 3-qubit quantum entanglement, characterized in topological terms, for quantum random number generation with publicly accessible proof of randomness, allowing an external party to freely and publicly verify the randomness of the generated sequence without disclosing of its secrecy or distorting it in any way (which is crucial for eventual applications in quantum and classical cryptography).

Keywords: quantum random number generator; QRNG; quantum entanglement; randomness; public verification of randomness, entanglement topology

1. Introduction

The essential character of quantum entanglement, a purely quantum concept, can be described as a non-local or thus global phenomenon. Discussion of non-locality of quantum entanglement has been very active since formulation of the EPR programme in 1935 [1,2]. Since then it became clear in the sixties, that quantum entanglement correlations in measurements violate classical limits imposed by statistical consideration [3]. There have long been discussed so called hidden-variables theories to complement for the seemingly missing elements of reality lacking in quantum mechanics description. But the Bell inequalities violation as well as the empirical confirmation by Aspect experiment [4], have ruled out the possibilities to address hypothetical variables as local. This resolves now to common understanding that quantum entanglement is essentially non-local if one is to sustain the realism assumption in science. As the property of non-locality lies in the center of interest of topology, it can be justified to search for some mathematical objects which can model the entanglement from the topological point of view. Such ideas were developed within last years, for example in Refs 5–7, as well as in recent conjectures based on the concept of entanglement being equivalent to curved space-time features of Einstein-Rosen Bridge [8,9]. In this work we aim to present some special aspects of quantum entanglement in a topological interpretation and discuss possible applications towards quantum random number generator (QRNG) [10].

On a very abstract level the most intuitive model of the entanglement between two quantum states (for simplicity we limit our consideration to most simple two-dimensional quantum states, which are referred to as qubits) seems to be the entanglement of two geometrical rings. Topological character of such rings resembles entanglement between two qubits—despite the space separation the quantum entanglement remains intact same as the entanglement of two rings regardless of their sizes. It should be noted, that links of fundamental aspects of quantum mechanics with topological description and in particular braid groups, are all well-known concepts, leading from the most obvious example to geometrical explanation of quantum statistics (distinction of fermions and bosons in 3D) by topological differences in trajectories for elementary particles quantum states replacements, as well as concept of anyons [11] in 2D physical systems and discussion of QHE (Quantum Hall Effect), where the paper authors have formulated own contributions [12–14].

In terms of the braid group for 2D plane [15] the elementary entanglement would be represented by a 2-braid of form σ_i^2, cf. Fig. 1 b)—two hooked rings. On the other hand, two unentangled qubits state would be represented by a trivial 2-braid, ε—two unentangled rings, cf. Fig. 1 a). However, such analogy is only able to describe the sole existence of the entanglement (hooked/entangled or unhooked/unentangled rings), while not the peculiarities of the modelled entanglement (e.g. differences between maximally entangled states in the Bell basis or the differences in a degree of entanglement between two qubits, such as $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |10\rangle)$).

Nevertheless, the topological braid group model allows to notice some fundamental distinguishment of entanglement types by their topological inequivalence when considering the entanglement of systems with 3 or more qubits. In a case of a 3-qubit system one can distinguish two topologically inequivalent entanglement types—the one corresponding to an entangled state, in which when any of 3 (or generally n) qubits is measured then 2 (or n-1) other qubits instantly become unentangled due to von Neumann projection and the algebraic structure of the quantum states tensor product linear combination (the Greenberger-Horne-Zeilinger GHZ state [16]), as well as the other type (a more W like state [17]) corresponding to such an entangled state of 3 (n) qubits configuration, in which after measuring of any of the 3 (n) qubits, the 2 (or n-1) others remain still entangled (in some Bell state selected arbitrarily, but correspondingly to the first qubit measurement outcome).

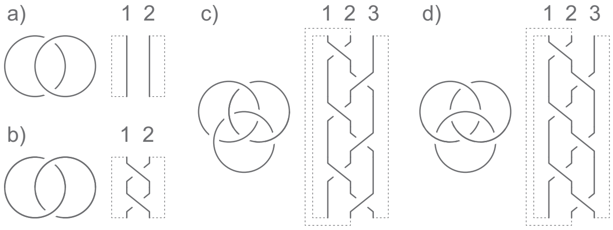

Figure 1. A simple topological model corresponding to inequivalence in terms of topology of the basic quantum entanglement types for two-dimensional quantum systems (qubits). As elements of the braid group are in fact closed loops, the gapped lines were added for clarity.

In case of the GHZ state, $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, or similar states, one can describe their topology (using the entangled rings model) in the form of the so called Borromean rings [18]. It is such rings arrangement that when cut open any of the rings the two remaining would always be unentangled.

In the braid group language such topology would correspond to 3-braid in form of $\sigma_1 \cdot \sigma_2^{-1} \cdot \sigma_1 \cdot \sigma_2^{-1} \cdot \sigma_1 \cdot \sigma_2^{-1}$, cf. Fig. 1 c).

A second (topologically inequivalent) type of entangled state of 3 qubits, is for e.g. $\frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)$, which in terms of entangled rings corresponds to a topology of closed 3-linked chain—after cutting open any of the chain loops the two remaining will still be entangled.

In the braid group language such a topology would correspond to 3-braid in form of $\sigma_1 \cdot \sigma_2 \cdot \sigma_1 \cdot \sigma_2 \cdot \sigma_1 \cdot \sigma_2$, cf. Fig. 1 d).

This topological inequivalence of above entanglement types, very evident in geometrical representation, is on the other hand not easily visible in the entanglement tensor product representation algebraic structure or within the entanglement generation process, which can be described formally for instance in the language of single and two qubits quantum gates (linear unitary operators in corresponding Hilbert spaces), as presented below.

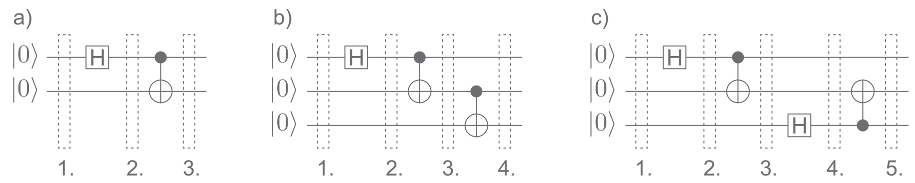

Figure 2. Exemplary basic quantum circuits schemas depicting topologically inequivalent entanglement types generation. Gapped regions depicts consecutive steps of quantum circuit evaluation.

Basic quantum circuits generating different entanglement types described above are depicted in Fig. 2. Basic evaluations of those quantum circuits are presented below for clarity:

- Fig. 2 a)—the Bell states generator—gapped regions evaluation:
  1. Initial state: $|0\rangle \otimes |0\rangle$
  2. After the Hadamard gate acting on qubit 1: $\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes |0\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right)$
  3. After the CNOT gate acting on qubits 1 and 2: $\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$
- Fig. 2 b)—the Borromean rings topology state generator (GHZ 3-qubit entanglement)—gapped regions evaluation:
  1. Initial state: $|0\rangle \otimes |0\rangle \otimes |0\rangle$
  2. After the Hadamard gate acting on qubit 1: $\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes |0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right) \otimes |0\rangle$
  3. After the CNOT gate acting on qubits 1 and 2: $\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \otimes |0\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |110\rangle\right)$
  4. After the CNOT gate acting on qubits 2 and 3: $\frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)$
- Fig. 2 c)—the closed 3-linked chain topology state generator—gapped regions evaluation:
  1. Initial state: $|0\rangle \otimes |0\rangle \otimes |0\rangle$
  2. After the Hadamard gate acting on qubit 1: $\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes |0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right) \otimes |0\rangle$
  3. After the CNOT gate on qubits 1 and 2: $\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \otimes |0\rangle$
  4. After the Hadamard gate acting on qubit 3: $\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \otimes \frac{1}{\sqrt{2}}|0\rangle + |1\rangle = \frac{1}{2}\left(|000\rangle + |001\rangle + |110\rangle + |111\rangle\right)$
  5. After the CNOT gate acting on qubits 3 and 2: $\frac{1}{2}\left(|000\rangle + |011\rangle + |110\rangle + |101\rangle\right)$

2. Randomness generator using entanglement

Differences between two mentioned types of three qubit entanglement states, characterized in topological terms with 3-link chain or Borromean rings topology, can be used to discuss distinct basic protocols in area of the quantum random number generators (QRNG) based on quantum entanglement.

Let us remind the form of the Bell basis:

$$\begin{aligned}
\Psi^{+}_{AB} &= \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right), \\
\Psi^{-}_{AB} &= \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} - |11\rangle_{AB}\right), \\
\Phi^{+}_{AB} &= \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} + |10\rangle_{AB}\right), \\
\Phi^{-}_{AB} &= \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} - |10\rangle_{AB}\right).
\end{aligned} \tag{1}$$

In a sense of quantum measurement, interpreted accordingly to probabilities represented by modulus squared of quantum superposition coefficient standing with the quantum state corresponding to measurement result and von Neumann projection postulate, those state can be grouped in two classes: the correlated and anti-correlated ones. States Ψ^+_{AB} and Ψ^-_{AB} are correlated in a specific way in sense of results of measurements of both qubits—if the first qubit is found in state $|0\rangle_A$ then the second qubit must be also in state $|0\rangle_B$, and similarly for state $|1\rangle$—this can be called type 1 of the entanglement (correlation of the measured states results). States Φ^+_{AB} and Φ^-_{AB} are in contrast correlated in a different manner—the result of the second measurement is always opposite to the result of the first measurement—type 2 of the entanglement (anti-correlation of the measured states results).

As to determine which type of correlation one deals with at the entangles state of 2 qubits, one must measure both qubits to get the classical information (measurement outcome) to identify the type of the correlation.

Let's consider those two distinct types of correlation within the Bell basis (correlation and anti-correlation) as a random results of the measurement of entangled 3-qubit state, characterized by a specific topological nature of its entanglement. This fundamental difference (correlation or anti-correlation) will be used to encode classical random bit in the sequence generated within such an entanglement based Quantum Random Number Generator protocol.

An example of such a 3-qubit state has the form $\frac{1}{2}\left(|000\rangle_{XAB} + |011\rangle_{XAB} + |101\rangle_{XAB} + |110\rangle_{XAB}\right)$. In terms of topological description of entanglement as a topology of rings, this state is represented by a closed 3-linked chain (each chain is linked with both others). In such a chain entanglement configuration it is possible to cut one of the rings of chain and remove it without cutting two remaining chain rings—those two rings will remain entangled. In the notion of above quantum state the cutting procedure can be identified with the measurement of one of 3 qubits in the computational basis (i.e. von Neumann projection of quantum information of this one qubit to classical bit information of either 0 or 1). But the process of cutting one of the chain rings can be carried out in two distinct ways, which correspond to two distinct results of measurement of one of the qubits rendering the measurement outcome to be 0 or 1. Different measurement results corresponds to qualitatively different joint entangled state of the two left qubits.

According to the above 3-qubits entangled state one can write

$$\frac{1}{2}\left(|000\rangle_{XAB} + |011\rangle_{XAB} + |101\rangle_{XAB} + |110\rangle_{XAB}\right) = \frac{1}{\sqrt{2}}|0\rangle_X \frac{|00\rangle_{AB} + |11\rangle_{AB}}{\sqrt{2}} + \frac{1}{\sqrt{2}}|1\rangle_X \frac{|01\rangle_{AB} + |10\rangle_{AB}}{\sqrt{2}}, \tag{2}$$

where the LHS of the equation is represented upon the Hilbert space in form $H_X \otimes H_A \otimes H_B$ and the RHS in form $H_X \otimes (H_A \otimes H_B)$.

The measurement of X qubit will lead to one of the two possible results with the same probability $\frac{1}{2}$. The resultant state $|0\rangle_X$ corresponds to the state $\frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right)$ and the resultant state $|1\rangle_X$ corresponds to the state $\frac{1}{\sqrt{2}}\left(|01\rangle_{AB} + |10\rangle_{AB}\right)$.

The above scheme can be represented in form of a quantum circuit, cf. Fig. 3.

Such a setup can be called an entanglement based random correlation generator. By continuously initiating the setup with state $|000\rangle_{XAB}$ and performing the measurement on auxiliary qubit X (or in fact on any other qubit) the setup will generate as an outcome, in a truly (non-deterministically quantum) random manner, the 2-qubit entanglement state in a specific correlation type, either fully correlated or fully anti-correlated (entanglement of qubit A and B if qubit X was measured).

2.1. Quantum random number generator with publicly verifiable randomness

As an extension of the above presented original concept in the field of QRNG, we now present a simple protocol, involving specific 3-qubit quantum entanglement characterized in topological terms, for quantum random number generation with publicly accessible proof of randomness, which is

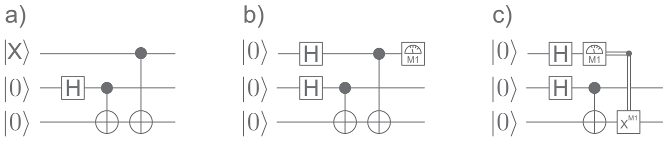

Figure 3. Quantum gate scheme of a random correlation entanglement generator with 2-qubit entanglement state and one auxiliary qubits X. Without (a) or with (b,c) a random selection of 2-qubit entangled state type. Double line represents classical information about the measurement result.

conceptually achieved on a fundamental (fraud-resistant) level for the first time. As quantum random number generators are gaining in popularity, especially with regard to possibility of a break-through with the efforts in construction of a scalable quantum computer that could endanger deterministic pseudo-randomness based on computational complexity, a protocol allowing for an external party to freely and fraud-proofly verifying of the true randomness of the generated sequence without distorting it in any way and most importantly without getting to know this very sequence by a party which is only interested in checking if the random sequence is truly random, seems to be of a potential use. In other words this protocol for the first time offers the generation of the random sequence with means to publicly prove the true randomness of the generated sequence without revealing this sequence, which would render it useless in different cryptographic applications. It should be noted that the previously considered QRNG protocols do not offer such mean of public verification of true randomness, and the randomness using party must rely on trust to the QRNG device supplier. The QRNG device based on the here proposed protocol is on the other hand publicly and objectively verifiable true randomness generator. It is worth to note that the public and objective verification of true randomness concerns in this protocol the very sequence of random bits that undergo desired randomness application, and thus when verified by any external party that these bits are truly random they are guaranteed to be so within a corresponding application without the need to reveal their values. This is in contrast to possible claims for other means of random bit sequences randomness verification, when for example random positions of the sequence are unveiled and their randomness publicly tested: in that case if the verification is positive it only guarantees to external parties that these very tested bits were random, but does not give any guarantee about the randomness of the remaining bits if one is not able to prove publicly the true randomness of the testing bits choice. In short the novelly proposed here QRNG protocol gives mean for universal randomness proof based on the fundamental correlation / anti-correlation of quantum entangled states distributed between protocol parties. In order to prevent attacks on the protocol based on the decreased measures of entanglement between the distributed qubits states (in essence with external eavesdropping qubits being co-entangled, thus taking the 3 or in general n qubit states out of their maximal and symmetrical entangled configurations) this QRNG protocol could be supplemented in the initial stage with well-known protocols of entanglement distillation and purification [19–21]).

One can consider the following formalization of the protocol, which we will call a quantum random number generator with public proof of randomness:

1. Let's assume that Alice owns generator described above.
2. Alice continuously initiate quantum setup from Fig. 3 with state $|000\rangle_{ABC}$.
3. After each initialization Alice performs a quantum measurement on qubit A, and keeps the result of each measurement in secret (this will be called a sequence A_i). Only Alice has the knowledge what type of entanglement was randomly chosen for each generated pair.
4. In result a continuous series of entangled pairs of B and C qubits are produced, with entanglement defined by elements of the sequence A_i (cf. Fig. 5), as follows
   - $0 \rightarrow \frac{|00\rangle_{BC}+|11\rangle_{BC}}{\sqrt{2}}$ – correlated state,
   - $1 \rightarrow \frac{|01\rangle_{BC}+|10\rangle_{BC}}{\sqrt{2}}$ – anticorrelated state.

5. Next Alice performs a measurement on qubits in each pair, which results in two bit sequences:
    - B_i – sequence of random bits resulting from measurements of qubit B from each pair,
    - C_i – sequence of random bits resulting from measurements of qubit C from each pair (in fact there is no need to perform qubit C measurements as the sequence B_i and the sequence A_i define their states unequivocally).
6. Alice ends with 3 equal length sequences:
    - sequence of entanglement type selected for each pair, A_i,
    - B_i and C_i – mutually correlated, by the sequence A_i, random sequences.

For someone who does not have any knowledge about the types of entanglement selected for each pair, sequences B_i and C_i are completely random and a prediction of the bits from one sequence (e.g. C_i) basing only on the second (B_i) sequence is in such case impossible. On the other hand, for Alice, from all those three sequences (B_i, C_i, and entanglement type selections sequence A_i) only two (and any arbitrary two) presents a random information.

But the most important thing is that any two sequences, e.g. B_i and C_i must have identical statistical properties (due to entanglement correlation or anticorrelation), and this feature is crucial here allowing Alice for the enhanced randomness verification.

As there is always a doubt whether the generated sequence is truly random or not, both in classical and quantum case (in the classical case this doubt can be addressed to the problem of the definition of the randomness itself, and in the quantum case it corresponds to the quantum mechanics interpretation differences between the von Neumann measurement concept based on an objective frequential probability and Fuchs Quantum Bayesianism theory, so called QBism, based on a rather subjective conditional probability [22,23], for example discussed in Ref. 24), statistical randomness testing offers some kind of verification. But the randomness testing suffers from a fundamental problem – lack of universal set of tests. In fact, there is an infinite number of different pattern matching tests, as there is an infinite number of patterns.

Therefore comprehensive testing can be highly resource consuming, and in general not available to be implemented in miniaturized quantum random number generator solutions. On the other hand a good quality randomness for a personal cryptographic usage (initial secrets, initialization vectors, nonces, etc.) is highly desirable. The proposed protocol can be used to transfer the weight of randomness testing from the generator device or the user to some external public party (which can have unlimited computational resources in comparison to a single user/generator).

In view of the above further steps of proposed protocol can realize the following use case scenario:

7. Alice doubting the randomness of the B_i sequence publicly sends the C_i sequence to the Verification Center (VC).
8. VC publicly performs a series of resource consuming randomness testing, deciding whether the sequence C_i can be considered truly random or not.
9. VC publicly informs Alice about its decision.
10. In case of a positive decision Alice gains the certainty that the sequence B_i remaining secret is also truly random.

In this protocol Alice can perform own initial randomness testing and use VC to enhance testing procedure. Due to the specific way of generation of sequences B_i and C_i, a public announcement of one of them does not affect the secrecy of the other one. The public character of VC randomness testing procedure serves as a warranty against fraud – decision of VC can be verified by any other public party (in general Alice can use multiple VCs simultaneously to increase the precision of the decision).

It is worth mentioning that VC can be possibly equipped with the quantum computer, which could be used to check whether the generation process is truly random or biased (for example, by the presence of a classical and thus deterministic influence on the generation process).

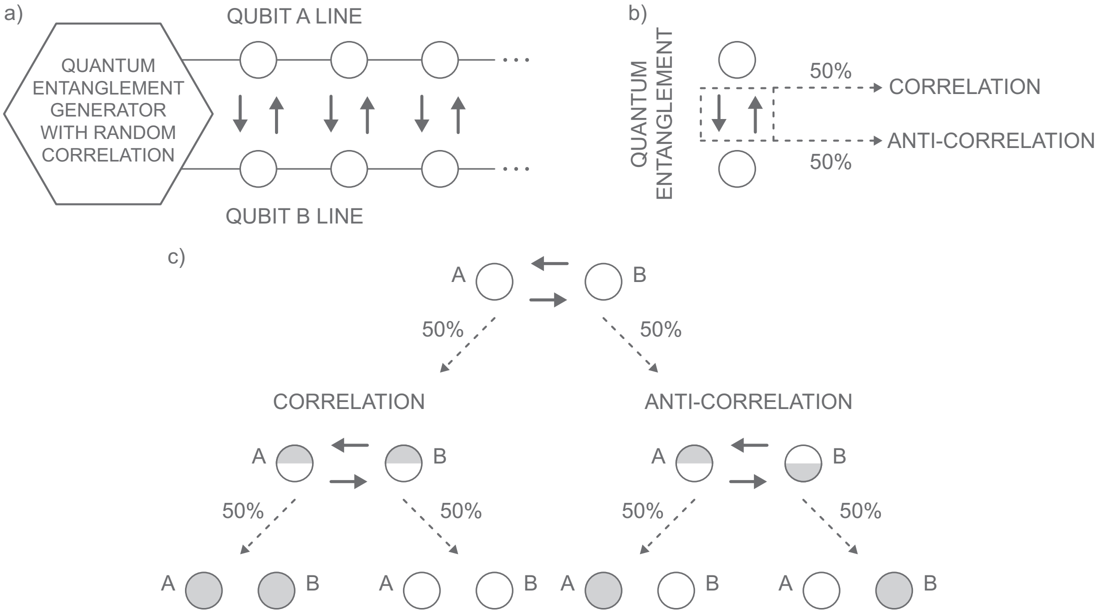

Figure 4. Schematic elements of protocol for quantum random number generator with public proof of randomness: a) generation of random correlations; b) correlation types; c) possible measurement outcomes.

Proposed protocol offers randomness certified by classical statistical tests performed publicly. Here the quantum randomness has a twin origin – quantum measurement choosing correlated or anticorrelated entangled state of a qubits pair, and measurement unentangling this pair. Alice, randomly performing verification of entanglement existence, tries to check whether the quantum source of entropy is of good quality or not. In this context it can be considered as a member of a wide class of so called Device Independent RNG [25,26], which are also verified statistically, as their generation process can be considered biased. In the proposed case, considered quantum randomness is based on a quantum measurement, but the bias can correspond here not only to implementations imperfections, as considered for the Device Independent RNG concept [25,26], but also to a non-trivial problem with introducing subjectivism to the quantum measurement due to questioning the correctness of using the frequentist probability in von Neumann measurement concept instead of conditional probability as described within the Quantum Bayesianism theory [22,23]. As the quantum measurement in its foundations is unrepeatable and destructive and No-Cloning theorem [27] applies, the concept to describe a measurement with a frequentist probability is somehow problematic. But regardless of the nature of the bias (either fundamental or implementation-wise), the proposed protocol allows to perform inaccessible in a standard case, due to computational inefficiency, simultaneously (with use of multiple VCs) randomness tests on large blocks of data (instead of rather short blocks in standard tests, for example NIST test suite [28]).

The problem of analyzing the entropy of the source of randomness is surely crucial for imperfect physical applications of quantum random generators (e.g. [26,29]). Some approaches are limited to specific generating techniques and setups [26,30,31]. More universal approaches are concepts of Device Independent RNG [25,32], where some of the protocols extract quantum randomness and discard deterministic behavior [33,34] due to quantum processes implementation shortcommings. Self-testing QRNG protocols are also considered as part of device independent approach, for example in Ref. 35, where testing of the dimension of uncharacterized classical and quantum systems allows the observer to separate the quantum part of the randomness from a deterministic classical part, which results with very high confidence of 99

2.2. GHZ-type states for quantum randomness

As mentioned previously, the Greenberger–Horne–Zeilinger (GHZ) [16] state is a specific type of a 3-qubit entangled state. It has a following form

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle_{ABC} + |111\rangle_{ABC}\right). \tag{3}$$

It is worth noting that if both discussed states, $|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)$ and $|\text{3-link chain}\rangle = \frac{1}{2}\left(|000\rangle + |011\rangle + |101\rangle + |110\rangle\right)$, were similarly used, as in discussed above protocol, the results, from point of view of the entropy, are quite different. If one of qubits in the series of GHZ states was measured in a computational base, then each time both other qubits are simultaneously unentangled in pure states and their measurements carry no entropy (the only entropy is within the first unentangling measurement). In the case of a series of 3-link chain states, to determine the classical states of each 3 entangled qubits, one needs to perform not one but two quantum unentangling measurements, what leads to twice as big entropy as in GHZ case. If one considers on the other hand the W state, defined as follows $|W\rangle = \frac{1}{\sqrt{3}}\left(|100\rangle + |010\rangle + |001\rangle\right)$, then in case of a series of measurements made on each first qubit in series of W states will lead to two different results, either all 3 qubit states are defined – first qubit is in state 1, or only the first qubit is defined in state 0 and the two other qubits stays in anticorrelated entangled state - in this case another unentangling measurement is needed to define classical state of all three qubits. Of course due to the above situation all 3 bit sequences will have non-uniform distributions of 0's and 1's (which is a consequence of the lack of binary symmetry in entanglement configuration of the W state). In terms of entropy, the series of measurements of qubits triples entangled in W states leads to entropy smaller than in GHZ states.

Generalized multiple GHZ state can be written as

$$|\mathrm{GHZ}\rangle^{(M)} = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes M} + |1\rangle^{\otimes M}\right), \tag{4}$$

where $M > 2$ is the number of qubits, and $|\alpha\rangle^{\otimes M}$ is a M-times tensor product of states $|0\rangle$.

One can say that GHZ-type states are a multiple-qubits generalization based on the structure of one of the Bell basis states of qubits entangled pair, the $\Psi^{+}_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right)$. In all of those states after the measurement each qubit is in the same state as all others. This property enables to consider another important feature for QRNG, namely the simultaneous generation of a random number string in all parties holding qubits which state were described by a GHZ-type state, which is referred as quantum secret sharing [32,36]. Such concept holds potentially important aspect for cryptography of secret communication, introducing extended concept of the Quantum Key Distribution (QKD) protocol (where all engaged in distribution parties trust an entanglement source), not hampered by point-to-point topology, which is often considered one of main drawbacks of quantum cryptography. The considered in detail multiparty QRNG protocol can be for example utilized to distribute securely (in terms of theoretical security guaranteed by quantum mechanics laws) a classical and fully random key (a random bit sequence) between multiple parties simultaneously, thus enabling symmetrically encoded secure broadcasting, or any other random numbers application which require the sequence to remain known only to engaged parties.

2.3. Generalization of randomness generator using entanglement

In case of the simplest scenario the GHZ entangled 3-qubit state can be considered with qubits A, B, C. After the first measurement of any of the qubits all of the 3 qubits will attain certain state depending on this measurement result due to the von Neumann projection postulate and GHZ state algebraical tensor product structure. Assuming continuous generation and distribution of the GHZ states, such procedure, if repeated consecutively, will generate 3 copies of a random sequence of classical information bits.

But in the case when one of the party will measure a single qubit which is in one of the below states, truly randomly selected,

$$\begin{aligned} &\frac{1}{\sqrt{2}}\left(|000\rangle_{ABC}+|111\rangle_{ABC}\right),\\ &\frac{1}{\sqrt{2}}\left(|001\rangle_{ABC}+|110\rangle_{ABC}\right),\\ &\frac{1}{\sqrt{2}}\left(|010\rangle_{ABC}+|101\rangle_{ABC}\right),\\ &\frac{1}{\sqrt{2}}\left(|011\rangle_{ABC}+|100\rangle_{ABC}\right), \end{aligned} \tag{5}$$

the results of measurements of other two qubits (of qubit B and C) will be totally independent from each other and from result of qubit A measurement.

The above states can be selected in a random manner by using of another two additional qubits, as follows.

5-qubits system can be organized to generate a random state from above set after being initialized by state $|00000\rangle_{XYABC}$, where qubits X and Y are auxiliary qubits. The quantum circuit setup state before the measurement of any of two auxiliary qubits states should be in the state

$$\begin{aligned} \psi_{XYABC} = &\frac{1}{2}|00\rangle_{XY}\frac{1}{\sqrt{2}}\left(|000\rangle_{ABC}+|111\rangle_{ABC}\right)\\ &+\frac{1}{2}|01\rangle_{XY}\frac{1}{\sqrt{2}}\left(|001\rangle_{ABC}+|110\rangle_{ABC}\right)\\ &+\frac{1}{2}|10\rangle_{XY}\frac{1}{\sqrt{2}}\left(|010\rangle_{ABC}+|101\rangle_{ABC}\right)\\ &+\frac{1}{2}|11\rangle_{XY}\frac{1}{\sqrt{2}}\left(|011\rangle_{ABC}+|100\rangle_{ABC}\right). \end{aligned} \tag{6}$$

According to above state ψ_{XYABC} after the measurements of qubits X and Y, the overall state of qubits A, B and C is defined, but in an entirely random manner, same as the two mentioned measurements results.

After the measurement of any single qubit of these three qubits, the states of the other two qubits will, in a random manner attain their respective values depending on the type of the entanglement.

Public announcement of one of the random sequences will not affect the security of random sequences.

Now Alice can verify the randomness of all sequences just by public announcement of one of them to the Verification Center (VC). All other, kept in secret, random sequences share the same statistical correlation as the one published and verified. In case of a positive assessment of the VC, the protocol leads to an interesting result – Alice certified twice the long random sequence as the sequence being tested for randomness.

This is an example of a generalization of the discussed above scheme for quantum random number generator with public proof of randomness. Only one sequence is required to be publicly exposed to be checked for randomness thus verifying the randomness of the other sequences, while all other sequences (in case of 3-qubit scheme only one sequence, in 5-qubit scheme 2 sequences, etc.) have the same statistical properties but their actual values stay undisclosed.

A quantum circuit scheme is depicted in Fig. 5. To achieve random selection of qubits A, B and C entangled state the 2 measurement gates are introduced, which control the single-qubit gates (measurement gates controlling other unitary quantum gates in quantum information circuit is a well-known approach, e.g. present in the circuit of the quantum teleportation [37]).

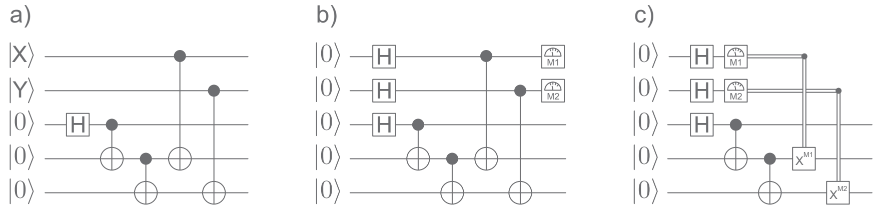

Figure 5. Quantum circuit scheme with gates of a random correlation entanglement generator with 3-qubit entanglement state and two auxiliary qubits X and Y. The generalization of the protocol (increased security of the multiple consent) is attained with the random selection of 3-qubits entangled state type, which is omitted in case (a) and included in cases (b,c). Double line represents classical information about the measurement result.

Similar setup can be proposed for higher number of entangled qubits. For clarity with the 4-qubits entangled state one will have

$$\begin{aligned}\psi_{XYZABCD} = &\frac{1}{2}\,|000\rangle_{XYZ}\,\frac{1}{\sqrt{2}}\,(|0000\rangle_{ABCD} + |1111\rangle_{ABCD})\\ + &\frac{1}{2}\,|001\rangle_{XYZ}\,\frac{1}{\sqrt{2}}\,(|0001\rangle_{ABCD} + |1110\rangle_{ABCD})\\ + &\frac{1}{2}\,|010\rangle_{XYZ}\,\frac{1}{\sqrt{2}}\,(|0010\rangle_{ABCD} + |1101\rangle_{ABCD})\\ + &\frac{1}{2}\,|011\rangle_{XYZ}\,\frac{1}{\sqrt{2}}\,(|0011\rangle_{ABCD} + |1100\rangle_{ABCD})\\ + &\frac{1}{2}\,|100\rangle_{XYZ}\,\frac{1}{\sqrt{2}}\,(|0100\rangle_{ABCD} + |1011\rangle_{ABCD})\\ + &\frac{1}{2}\,|101\rangle_{XYZ}\,\frac{1}{\sqrt{2}}\,(|0101\rangle_{ABCD} + |1010\rangle_{ABCD})\\ + &\frac{1}{2}\,|110\rangle_{XYZ}\,\frac{1}{\sqrt{2}}\,(|0110\rangle_{ABCD} + |1001\rangle_{ABCD})\\ + &\frac{1}{2}\,|111\rangle_{XYZ}\,\frac{1}{\sqrt{2}}\,(|0111\rangle_{ABCD} + |1000\rangle_{ABCD}),\end{aligned} \tag{7}$$

where qubits X, Y and Z are auxiliary qubits for setting random state of 4 qubits A, B, C and D.

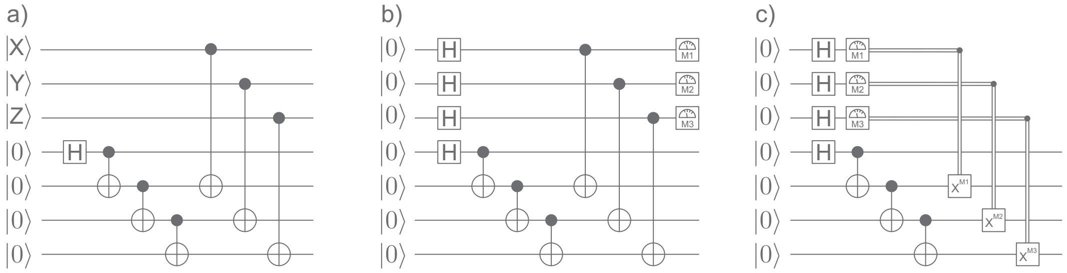

Figure 6. Quantum gate scheme of a random correlation entanglement generator with 4-qubits entanglement state and three auxiliary qubits X, Y and Z. Without (a) and with (b,c) random selection of 4-qubits entangled state type. Double line represents classical information about the measurement result.

The measurement of 3 auxiliary qubits results in arrangement, in a truly random manner (guaranteed by the fundamentally non-deterministic quantum measurement property), of a specific type of the 4 qubits entanglement.

One can also consider different setup, this time consisting of four qubits, A, B, C and D, initiated in the following state:

$$\begin{aligned}\Psi_{ABCD} =& \frac{1}{2\sqrt{2}} |0\rangle_A \left(|000\rangle_{BCD} + |011\rangle_{BCD} + |101\rangle_{BCD} + |110\rangle_{BCD}\right) \\ +& \frac{1}{2\sqrt{2}} |1\rangle_A \left(|111\rangle_{BCD} + |100\rangle_{BCD} + |010\rangle_{BCD} + |001\rangle_{BCD}\right).\end{aligned} \tag{8}$$

The measurement in this entangled four qubit state of the qubit A will lead to one of two possible 3-link chain states for qubits B, C and D. Next measurement on any of those three remaining qubits (for example qubit B) will choose appropriate entangled state for 2 remaining qubits, C and D. Final measurement of one of the C and D qubits set their states (all three measurements are considered in computational basis, similarly as all mentioned measurements in this paper). Iterating of such procedure for series of states Ψ_{ABCD} will result in 4 sequences, where 3 are independent, similarly as in the beginning of this section.

3. Conclusions

Presented above propositions for a family of protocols for extended quantum random number generators are based on multi-qubit entanglement properties. In view of the current development in experimental physics, the requirements of presented schemes can already be technologically met and the above originally proposed protocols can be implemented. Generally the QRNGs are currently considered to be in the stage of industry adoption technology level (there are commercial companies already selling production QRNG devices, which hold one key advantage over RNGs based on classical in contrast to quantum physical effects, i.e. fundamentally non-deterministic randomness, which is impossible to predict due to quantum mechanical laws, no matter what technology used).

In 2016, an experimental setup for generation for the ten-photon polarization entanglement with use of BBO (beta-barium borate) crystals was presented, cf. Ref. [38], opening new area for the quantum engineering. On the plane of possible applications the proposed novel QRNG protocols, i.e. quantum random number generator with publicly verifiable randomness, with their discussed generalizations might be of a significance for cryptography and secure communications (including also problems of authentication), as they introduce new important properties. The main advantage in contrast to standard QRNG protocol is that all previously considered schemes did not offer any mean of public verification of true randomness. This is very critical issue in terms of applications as potential users of QRNGs must rely on trust assumption, not being able to offer verification of the very randomness used without revealing it. The originally proposed here QRNG protocol can be basis for a device that will enable objective verification of the true randomness of the used bit sequence, without disposing of its secrecy. As the measurement setups for each single qubit in the above schemes can be implemented with use of one polarization beam-splitters and two single-photon detectors and the quantum gates for polarization encoded qubits are also widely available and rapidly developed, with currently ongoing implementations of integrated gates (e.g. cf. Refs [39,40]), it is worth pointing out that the discussed protocols are within the reach of practical implementations.

On the other hand on the level of theoretical considerations, it should be summarized that the new important properties discussed in the above proposed protocols, are strongly linked with multiple qubits entangled states and their topological features. The topology related nature of quantum entanglement is currently a hot topic of consideration relating the links between quantum mechanics and relativity, being revisited in the efforts of the Grand Unification of physical theories [41,42]. Understanding of how quantum entanglement manifests its non-local peculiar properties, or as Einstein called it, the spooky action over a distance, violating (empirically verified [2,4]) the local realism assumptions of classical physics, is certainly not yet achieved. But in terms of recent progress [43–48] topology (with links to direct topology of space-time) may be considered one of the most promising directions. In that regards studying topological properties of non-trivial quantum entanglement configurations is important, and as shown in the present paper can to lead identification of important practical features, that can be then used as a basis for definition of new quantum information processing and communication applications, such as the demonstrated novel QRNG protocols with publicly verifiable randomness. In this view perhaps of some interest is also the property of the proposed generalized entanglement QRNG protocols (with four or more entangled qubits) to use shorter sequences of random bits verified statistically to be truly random in order to information theoretically certify same randomness of longer sequences of bits remaining secret.

Acknowledgments: This work has been supported by the Polish National Centre for Research and Development within the project funded upon the Smart Growth Operational Programme POIR 1.1.1 (JURAND POIR.01.01.01-00-0173/15-00).

Author Contributions: All authors contributed equally to this work, both in intellectual aspect and writing of this paper.

Conflicts of Interest: The authors declare no conflict of interest.

1. Einstein, A.; Podolsky, B.; Rosen, N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev.* **1935**, *47*, 777–780. DOI: https://doi.org/10.1103/PhysRev.47.777.
2. Aspect, A.; Grangier, P.; Roger, G. Experimental Realization of Einstein–Podolsky–Rosen–Bohm Gedankenexperiment: A New Violation of Bell's Inequalities. *Phys. Rev. Lett.* **1982**, *49*, 91–94. DOI: https://doi.org/10.1103/PhysRevLett.49.91.
3. Bell, J. On the Einstein Podolsky Rosen Paradox. *Physics* **1964**, *1*, 195–200.
4. Aspect, A.; Grangier, P.; Roger, G. Experimental Tests of Realistic Local Theories via Bell's Theorem. *Phys. Rev. Lett.* **1981**, *47*, 460–463. DOI: https://doi.org/10.1103/PhysRevLett.47.460.
5. Aravind, P.K. Borromean entanglement of the GHZ state. In *Potentiality Entanglement and Passion-at-a-Distance: Quantum Mechanical Studies for Abner Shimony*; R. S. Cohen, M.H.; Stachel, J., Eds.; Kluwer Academic Publishers: Dordrecht, 1997; pp. 53–59. ISBN: 978-0-7923-4454-4.
6. Kauffman, L.H.; Lomonaco Jr, S.J. Quantum entanglement and topological entanglement. *New J. Phys.* **2002**, *4*, 73.1–73.18. DOI: https://doi.org/10.1088/1367-2630/4/1/373.
7. Sugita, A. Borromean Entanglement Revisited. *ArXiv e-prints* **2007**. arXiv:quant-ph/0704.1712 http://adsabs.harvard.edu/abs/2007arXiv0704.1712S.
8. Einstein, A.; Rosen, N. The Particle Problem in the General Theory of Relativity. *Phys. Rev.* **1935**, *48*, 73–77. DOI: https://doi.org/10.1103/PhysRev.48.73.
9. Morris, M.S.; Thorne, K.S.; Yurtsever, U. Wormholes, Time Machines, and the Weak Energy Condition. *Phys. Rev. Lett.* **1988**, *61*, 1446–1449. DOI: https://doi.org/10.1103/PhysRevLett.61.1446.
10. Schmidt, H. Quantum-Mechanical Random-Number Generator. *J. Appl. Phys.* **1970**, *41*, 462–468. DOI: https://doi.org/10.1063/1.1658698.
11. Wilczek, F. Quantum Mechanics of Fractional-Spin Particles. *Phys. Rev. Lett.* **1982**, *49*, 957–959. DOI: https://doi.org/10.1103/PhysRevLett.49.957.
12. Jacak, J.; Jóźwiak, I.; Jacak, L. New implementation of composite fermions in terms of subgroups of a braid group. *Phys. Lett. A* **2009**, *374*, 346–350. DOI: https://doi.org/10.1016/j.physleta.2009.10.075.
13. Jacak, J.; Gonczarek, R.; Jacak, L.; Jóźwiak, I. *Application of braid groups in 2D Hall system physics: composite fermion structure*; WorldScientific: Singapore, 2012. ISBN: 978-981-4412-02-5.
14. Jacak, J. Unconventional fractional quantum Hall efect in bilayer graphene. *Sci. Rep.* **2017**, *7*, 8720–1–13. DOI: https://doi.org/10.1038/s41598-017-09166-5.
15. Birman, J.S. *Braids, Links and Mapping Class Groups (AM-82), Volume 82*; Princeton UP: Princeton, 1974. ISBN: 978-069-1081-49-6.

16. Greenberger, D.M.; Horne, M.A.; Zeilinger, A. Going Beyond Bell's Theorem. In *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*; Kafatos, M., Ed.; Kluwer Academic Publishers: Dordrecht, 1989; pp. 69–72. ISBN: 978-94-017-0849-4.
17. D ur, W.; Vidal, G.; Cirac, J.I. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A* **2000**, *62*, 062314–1–12. DOI: https://doi.org/10.1103/PhysRevA.62.062314.
18. Cromwell, P.R.; Beltrami, E.; Rampichini, M. The Borromean Rings. *Math. Intelligencer* **1998**, *20*, 53–62. DOI: https://doi.org/10.1007/BF03024401.
19. Bennett, C.; Bernstein, H.; Popescu, S.; Schumacher, B. Concentrating Partial Entanglement by Local Operations. *Phys. Rev. A* **1996**, *53*, 2046–2052. DOI: https://doi.org/10.1103/PhysRevA.53.2046.
20. Bennett, C.; Brassard, G.; Popescu, S.; Schumacher, B.; Smolin, J.; Wooters, W. Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels. *Phys. Rev. Lett.* **1996**, *76*, 722–725. DOI: https://doi.org/10.1103/PhysRevLett.76.722.
21. Bennett, C.; DiVincenzo, D.D.; Smolin, J.; Wooters, W. Mixed State Entanglement and Quantum Error Correction. *Phys. Rev. A* **1996**, *54*, 3824–3851. DOI: https://doi.org/10.1103/PhysRevA.54.3824.
22. Mermin, N.D. Physics: QBism puts the scientist back into science. *Nature* **2014**, *507*, 421–423. DOI: https://doi.org/10.1038/507421a.
23. Fuchs, C.A.; Schack, R. Quantum-Bayesian coherence. *Rev. Mod. Phys.* **2013**, *85*, 1693–1715. DOI: https://doi.org/10.1103/RevModPhys.85.1693.
24. Khrennikov, A. Randomness: quantum versus classical. *Int. J. Quantum Inform.* **2016**, *14*, 1640009. DOI: https://doi.org/10.1142/S0219749916400098.
25. Pivoluska, M.; Plesch, M. Device Independent Random Number Generation. *Acta Phys. Slovaca.* **2014**, *64*, 600–663. DOI: https://doi.org/10.2478/apsrt-2014-0006.
26. Ma, X.; Yuan, X.; Cao, Z.; Qi, B.; Zhang, Z. Quantum random number generation. *Quantum Inf.* **2016**, *2*, 16021. DOI: https://doi.org/10.1038/npjqi.2016.21.
27. Wootters, W.K.; Zurek, W.H. A single quantum cannot be cloned. *Nature* **1982**, *299*, 802–803. DOI: https://doi.org/10.1038/299802a0.
28. Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E.; Leigh, S.; Levenson, M.; Vangel, M.; Banks, D.; Heckert, A.; Dray, J.; Vo, S. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. *Natl. Inst. Stand. Technol. Spec. Publ.* **2010**. 800-22rev1a http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf.
29. Nisan, N.; Ta-Shma, A. Extracting randomness: a survey and new constructions. *J. Comp. Sys. Sci.* **1999**, *58*, 148–173. DOI: https://doi.org/10.1006/jcss.1997.1546.
30. Frauchiger, D.; Renner, R.; Troyer, M. True randomness from realistic quantum devices. *ArXiv e-prints* **2013**. arXiv:quant-ph/1311.4547 http://adsabs.harvard.edu/abs/2013arXiv1311.4547F.
31. Ma, X.; Xu, F.; Xu, H.; Tan, X.; Qi, B.; Lo, H.K. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Phys. Rev. A* **2013**, *87*, 062327. DOI: https://doi.org/10.1103/PhysRevA.87.062327.
32. Shenoy-Hejamadi, A.; Pathak, A.; Radhakrishna, S. Quantum Cryptography: Key Distribution and Beyond. *Quanta* **2017**, *6*, 1–47. DOI: https://doi.org/10.12743/quanta.v6i1.57.
33. Pironio, S.; Acín, A.; Massar, S.; de la Giroday, A.B.; Matsukevich, D.N.; Maunz, P.; Olmschenk, S.; Hayes, D.; Luo, L.; Manning, T.A.; Monroe, C. Random numbers certified by Bell's theorem. *Nature* **2010**, *464*, 1021–1024. DOI: https://doi.org/10.1038/nature09008.
34. Christensen, B.G.; McCusker, K.T.; Altepeter, J.B.; Calkins, B.; Gerrits, T.; Lita, A.E.; Miller, A.; Shalm, L.K.; Zhang, Y.; Nam, S.W.; Brunner, N.; Lim, C.C.W.; Gisin, N.; .; Kwiat, P.G. Detection-Loophole-Free Test of Quantum Nonlocality, and Applications. *Phys. Rev. Lett.* **2013**, *111*, 130406. DOI: https://doi.org/10.1103/PhysRevLett.111.130406.
35. Lunghi, T.; Brask, J.B.; Lim, C.C.W.; Lavigne, Q.; Bowles, J.; Martin, A.; Zbinden, H.; .; Brunner, N. Self-Testing Quantum Random Number Generator. *Phys. Rev. Lett.* **2015**, *114*, 150501. DOI: https://doi.org/10.1103/PhysRevLett.114.150501.
36. Hillery, M.; Bužek, V.; Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **1999**, *59*, 1829–1834. DOI: https://doi.org/10.1103/PhysRevA.59.1829.
37. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information: 10th Anniversary Edition*; Cambridge University Press: Cambridge, 2010. ISBN: 978-110-7002-17-3.

38. Wang, X.L.; Chen, L.K.; Li, W.; Huang, H.L.; Liu, C.; Chen, C.; Luo, Y.H.; Su, Z.E.; Wu, D.; Li, Z.D.; Lu, H.; Hu, Y.; Jiang, X.; Peng, C.Z.; Li, L.; Liu, N.L.; Chen, Y.A.; Lu, C.Y.; Pan, J.W. Experimental Ten-Photon Entanglement. *Phys. Rev. Lett.* **2016**, *117*, 210502–1–6. DOI: https://doi.org/10.1103/PhysRevLett.117.210502.
39. Crespi, A.; Ramponi, R.; Osellame, R.; Sansoni, L.; Bongioanni, I.; Sciarrino, F.; Vallone, G.; Mataloni, P. Integrated photonics quantum gates for polarization qubits. *Nat. Commun.* **2011**, *2*, 566–1–6. DOI: https://doi.org/10.1038/ncomms1570.
40. Sansoni, L. Quantum Computation: Integrated Quantum Gates for Polarization Encoded Qubits. In *Integrated Devices for Quantum Information with Polarization Encoded Qubits*; Springer: Cham, 2014; pp. 57–63. ISBN: 978-3-319-07102-2.
41. Ross, G. *Grand Unified Theories (Frontiers in Physics)*; Westview Press: Boulder, 1984.
42. Georgi, H.; Glashow, S. Unity of All Elementary Particle Forces. *Phys. Rev. Lett.* **1974**, *32*, 438–441. DOI: https://doi.org/10.1103/PhysRevLett.32.438.
43. Van Raamsdonk, M. Building up spacetime with quantum entanglement. *Gen. Rel. Grav.* **2010**, *42*, 2323–2329. DOI: https://doi.org/10.1007/s10714-010-1034-0.
44. Swingle, B. Entanglement renormalization and holography. *Phys. Rev. D* **2012**, *86*, 065007–1–8. DOI: https://doi.org/10.1103/PhysRevD.86.065007.
45. Pastawski, F.; Yoshida, B.; Harlow, D.; Preskill, J. Holographic quantum error-correcting codes: toy models for the bulk/boundary correspondence. *J. High Energ. Phys.* **2015**, *2015*, 149. DOI: https://doi.org/10.1007/JHEP06(2015)149.
46. Stanford, D.; Susskind, L. Complexity and shock wave geometries. *Phys. Rev. D* **2014**, *90*, 126007–1–11. DOI: https://doi.org/10.1103/PhysRevD.90.126007.
47. Cowen, R. The quantum source of space-time. *Nature* **2015**, *527*, 290–293. DOI: https://doi.org/10.1038/527290a.
48. Susskind, L. Copenhagen vs Everett, Teleportation, and ER=EPR. *Fortschritte der Physik* **2016**, *64*, 551–564. DOI: https://doi.org/10.1002/prop.201600036.

© 2017 by the authors. Submitted to *Entropy* for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).