Three criteria for quantum random-number generators based on beam splitters

Karl Svozil*
Institute for Theoretical Physics, Vienna University of Technology, Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria
(Received 16 March 2009; published 15 May 2009)

We propose three criteria for the generation of random digital strings from quantum beam splitters: (i) three or more mutually exclusive outcomes corresponding to the invocation of three- and higher-dimensional Hilbert spaces, (ii) the mandatory use of pure states in conjugated bases for preparation and detection, and (iii) the use of entangled singlet (unique) states for elimination of bias.

DOI: 10.1103/PhysRevA.79.054306 PACS number(s): 03.67.Hk, 03.65.Ud, 05.40.−a

Quantum random-number generators are important for quantum-information processing as they are likely to be one of the first technologies applied for various physical and commercial applications. They also serve as components of other quantum devices for quantum key distribution and experiments testing and utilizing quantum nonlocality.

Randomness is a notorious property, both from theoretical and practical points of view. It is commonly accepted that there is a satisfactory definition [1] of *infinite* random sequences in terms of algorithmic incompressibility [2] as well as of the equivalent statistical tests [3]. Besides the obvious fact that all computable and physically operational entities are limited to *finite* objects and methods, algorithmic pseudorandom generators suffer from von Neumann's verdict that [4] "*anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin*." The halting probability Ω [5] shares three perplexing properties: it is computably enumerable (computable in a weak sense), provable random (which implies that Ω is noncomputable), as well as infinitely knowledgeable in its role as a "rosetta stone" for all decision problems encodable as halting problems [1]. A few of its starting bits have been computed [6], yet due to its randomness only finitely many bits of this number can ever be computed.

From the numerous random-number generators based on physical processes (cf. Refs. [7–12] to name a few), the use of single photons (or other quanta such as neutrons) subjected to beam splitters appears particularly promising [13–16] for the following reasons: (i) due to (ideally) single-photon events, the physical systems are "elementary;" (ii) they can be controlled to a great degree; and (iii) they can be certified to be random relative to the postulates of quantum theory [17].

Three features of quantum theory directly relate to random sequences generated from beam splitter experiments: (i) the randomness of individual events (cf. Ref. [18], p. 866 and Ref. [19], p. 804]); (ii) complementarity ([20], p. 7); and (iii) value indefiniteness, i.e., the absence of two-valued states interpretable as "global" (i.e., valid on all observables) truth functions [21]. In order to fully implement these quantum features, we propose three improvements to existing protocols [13–16,22–24].

The first criterion ensures that the quantum random-number generators can be certified to be subjected to quantum value indefiniteness. A necessary condition for this to apply is the possibility of *three or more mutually exclusive outcomes* in measurements of single quanta. Formally, this is due to the fact that violations of Bell-type inequalities, as well as proofs of Gleason's and Kochen-Specker-type theorems are only realizable [25] in three- and higher-dimensional Hilbert spaces. Only from three-dimensional vector space onward it is possible to nontrivially interconnect bases through one (or up to $n-2$ for n-dimensional Hilbert space) common base element(s). This can be explicitly demonstrated by certain, even dense [26–28], "dilutions" of bases, which break up the possibility to interconnect, thus allowing value definiteness. In more operational terms, if some "exotic" scenarios (e.g., Refs. [29,30]) are excluded, the violation of Bell-type inequalities for two two-state particles (corresponding to two outcomes on each side) is a sufficient criterion for quantum value indefiniteness.

Of course, one could argue that protocols based on two outcomes are still protected by quantum complementarity, and the full range of quantum indeterminism, in particular quantum value indefiniteness, is not needed. There is also the possibility that the Born rule might be derived through some other argument (possibly from another set of axioms) than Gleason's theorem [31–34]. However, there exist sufficiently many two-valued states on propositional structures with two outcomes to allow for a homeomorphic embedding of this structure into a classical Boolean algebra. In any case, it appears prudent to use all the "mind-boggling" features of quantum mechanics against cryptananalytic attacks on some quantum-generated sequence.

The resulting trivalent or multivalued sequence can be easily "downgraded" or "translated" to binary sequences through elimination or identification without loss of randomness: systematically eliminating $n-2$ symbol(s) will transform a random sequence on an alphabet with $n \geq 3$ symbols into a random sequence on an alphabet with two symbols [1].

The second criterion proposes the mandatory use of *pure* states from maximally conjugated bases for preparation and detection. This requirement deals with the *single-particle source* of quantum random-number generators. Indeed, many two-particle experiments have been using this criterion already, as full tomography is performed to characterize the state as completely as possible. These experiments use a (Bell) state which is as pure and maximally entangled as operationally feasible; quite often they produce the singlet Bell state (which, due to technical issues related to other

*svozil@tuwien.ac.at; http://tph.tuwien.ac.at/~svozil

degrees of freedom, can never be ideally pure). Tomography is used to characterize the state and hence certify the randomness of outcomes. Hence in this sense and in these experiments, the criterion is already implicitly implemented.

Although it is generally believed that mixed (nonpure) quantum states can be "produced" and operationalized "for all practical purposes," one might cautiously argue that this may actually be a subjective statement on behalf of the observer: whereas the experimenter might "pretend" that the exact state leaving the particle source is unknown, it might still be possible to conceive of the state to be in some, albeit unknown but not principally unknowable, unique pure state. This is related to the question of whether or not mixed states should be thought of as merely subjective constructions which even in the epistemic view—as the wave function (the quantum state) representing a catalog of expectations [35]—represent only certain partial incomplete representations of systems which might be completely defined by a single unique context.

Even if one is unwilling to accept these principal concerns, it remains prudent not to expose the protocols for generating quantum randomness to the possibility of hidden regularities of the source. After all, beam splitters are just one-to-one bijective devices representable by reversible unitary operators [36–38]—a fact which can be seen by recombining the two paths by a second beam splitter in a Mach-Zender interferometer, thereby recovering the original signal. Thus, in order to assure quantum randomness, the beam splitter should not be considered as an isolated element but has to be examined in combination with the source. In accordance with this principle, a *mismatch* between state preparation and measurement guarantees that quantum complementarity ensures the indeterministic outcome. This can, for instance, be implemented by preparing the single particle in a pure state which corresponds to an element of a certain basis and then measuring it in a different basis, in which the original state is in a coherent superposition of more than one states (cf. Ref. [13] and the first protocol using beam splitting polarizers in Ref. [15]).

Third and finally, in order to eliminate any possible bias (for some "classical" methods to eliminate bias, we refer to Refs. [39–42]), we propose to utilize Einstein-Podolsky-Rosen-type measurements of two quanta in a unique entangled state. Any state satisfying the uniqueness property [43] in at least two directions, such as the singlet states $\frac{1}{\sqrt{2}}(|\frac{1}{2},-\frac{1}{2}\rangle-|-\frac{1}{2},\frac{1}{2}\rangle)$, $\frac{1}{\sqrt{3}}(-|0,0\rangle+|-1,1\rangle+|1,-1\rangle)$, or $\frac{1}{2}(|\frac{3}{2},-\frac{3}{2}\rangle-|-\frac{3}{2},\frac{3}{2}\rangle-|\frac{1}{2},-\frac{1}{2}\rangle+|-\frac{1}{2},\frac{1}{2}\rangle)$ of two spin-$\frac{1}{2}$, -1, or -$\frac{3}{2}$ particles could be used for this purpose. In that way, the outcome of one particle can be combined with the outcome of the other particle to eliminate bias. Again, it should be kept in mind that physical realizations of this protocol can never be made ideal and necessarily suffer from, for instance, the nonideal behavior of the beam splitters.

For the sake of demonstration, suppose Alice and Bob share successive pairs of quanta in the singlet Bell state $\frac{1}{\sqrt{2}}(|\frac{1}{2},-\frac{1}{2}\rangle-|-\frac{1}{2},\frac{1}{2}\rangle)$. Denote Alices's and Bob's outcomes in the jth measurement by a_j and b_j, with the coding $a_j,b_j \in \{0,1\}$, respectively. Using XOR operations on their combined results by a product mod 2 of a_j and b_j, i.e., by defining $s_j=a_j\oplus b_j=a_jb_j \mod 2$, yields a totally unbiased sequence s_j of bits. Remarkably, as the state guarantees a 50:50 occurrence of 0's and 1's on either side, the associated bases of Alice and Bob need not even be maximally "apart:" one outcome on Alice's side can be thought of as serving as "one-time pad" in encrypting the other outcome on Bob's side, and vice versa. Again, this method will be as good as the entangled particle source. In order to eliminate causal influences, the events recorded by Alice and Bob should be separated by strict Einstein locality conditions [44,45], although separating the particles will be experimentally challenging.

Alternatively, in an adaptive "delayed choice" experiment the outcome on Alice's side could be transferred to Bob, who adjusts his experiment (e.g., by changing the direction of spin-state measurements) according to Alice's input [46]. This method resembles the previously implemented self-calibration techniques utilizing coincidence measurements [22], entropy measures [24], and iterative sampling [23]. Whether or not it could also be used for classical angular-momentum zero states "exploding" into two parts [47] remains unknown.

In summary we have argued that the present protocols for generating quantum random sequences with beam splitters should be improved to be certifiable against value definiteness and hidden bias of the source. We have also proposed a procedure to eliminate bias by using one particle of a singlet in an Einstein-Podolsky-Rosen configuration as a one-time pad for the other particle.

The author gratefully acknowledges discussions with and suggestions by Cristian Calude, as well as the kind hospitality of the Centre for Discrete Mathematics and Theoretical Computer Science (CDMTCS) of the Department of Computer Science at The University of Auckland. This work was also supported by The Department for International Relations of the Vienna University of Technology.

[1] C. Calude, *Information and Randomness—An Algorithmic Perspective*, 2nd ed. (Springer, Berlin, 2002).

[2] G. J. Chaitin, IBM J. Res. Dev. **21**, 350 (1977); *Information, Randomness and Incompleteness*, 2nd ed. (World Scientific, Singapore, 1990).

[3] P. Martin-Löf, Inf. Control. **9**, 602 (1966).

[4] J. von Neumann, in *John von Neumann, Collected Works*, edited by A. H. Traub (MacMillan, New York, 1963), Vol. V, p. 768.

[5] G. J. Chaitin, *Exploring Randomness* (Springer Verlag, London, 2001).

[6] C. S. Calude and M. J. Dinneen, Int. J. Bifurcation Chaos **17**,

1937 (2007).
[7] The RAND Corporation, Knolls Atomic Power Laboratory Report No. KAPL-3147, 1955 (unpublished). The data digits are obtainable via http://www.rand.org/pubs/monograph_reports/2005/digits.txt.zip, the introduction via http://www.rand.org/pubs/monograph_reports/MR1418/index2.html, http://www.rand.org/pubs/monograph_reports/MR1418/.
[8] C. H. Vincent, J. Phys. E **3**, 594 (1970).
[9] T. Erber and S. Putterman, Nature (London) **318**, 41 (1985).
[10] H. Schmidt, J. Appl. Phys. **41**, 462 (1970).
[11] A. J. Martino and G. M. Morris, Appl. Opt. **30**, 981 (1991).
[12] J. Walker, *Hotbits Hardware* (1986–2009), http://www.fourmilab.ch/hotbits/hardware3.html
[13] K. Svozil, Phys. Lett. A **143**, 433 (1990).
[14] J. G. Rarity, M. P. C. Owens, and P. R. Tapster, J. Mod. Opt. **41**, 2435 (1994).
[15] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675 (2000).
[16] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, J. Mod. Opt. **47**, 595 (2000).
[17] A. Zeilinger, Nature (London) **438**, 743 (2005).
[18] M. Born, Z. Phys. **37**, 863 (1926).
[19] M. Born, Z. Phys. **38**, 803 (1926).
[20] W. Pauli, in *Handbuch der Physik, Band V, Teil 1, Prinzipien der Quantentheorie I*, edited by S. Flügge (Springer, Berlin, 1958), pp. 1–168.
[21] S. Kochen and E. P. Specker, J. Math. Mech. **17**, 59 (1967); reprinted in works of E. Specker, *Selecta* (Birkhäuser Verlag, Basel, 1990), pp. 235–263.
[22] M. Hai-Qiang, W. Su-Mei, Z. Da, C. Jun-Tao, J. Ling-Ling, H. Yan-Xue, and W. Ling-An, Chin. Phys. Lett. **21**, 1961 (2004).
[23] P. X. Wang, G. L. Long, and Y. S. Li, J. Appl. Phys. **100**, 056107 (2006).
[24] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, Phys. Rev. A **75**, 032334 (2007).
[25] K. Svozil and J. Tkadlec, J. Math. Phys. **37**, 5380 (1996).
[26] C. D. Godsil and J. Zaks, University of Waterloo Research Report No. CORR 88-12, 1988 (unpublished).
[27] D. A. Meyer, Phys. Rev. Lett. **83**, 3751 (1999).
[28] H. Havlicek, G. Krenn, J. Summhammer, and K. Svozil, J. Phys. A **34**, 3071 (2001).
[29] I. Pitowsky, Phys. Rev. Lett. **48**, 1299 (1982).
[30] I. Pitowsky, Phys. Rev. D **27**, 2316 (1983).
[31] A. M. Gleason, J. Math. Mech. **6**, 885 (1957).
[32] I. Pitowsky, J. Math. Phys. **39**, 218 (1998).
[33] F. Richman and D. Bridges, J. Funct. Anal. **162**, 287 (1999).
[34] A. Dvurečenskij, *Gleason's Theorem and Its Applications* (Kluwer Academic Publishers, Dordrecht, 1993).
[35] E. Schrödinger, Naturwiss. **23**, 807 (1935); translated in English by J. D. Trimmer, Proc. Am. Philos. Soc. **124**, 323 (1980); http://www.tu-harburg.de/rzt/rzt/it/QM/cat.html; reprinted in works of J. A. Wheeler and W. H. Zurek, *Quantum Theory and Measurement* (Princeton University Press, Princeton, NJ, 1983), pp. 152–167.
[36] Z. Ou, C. Hong, and L. Mandel, Opt. Commun. **63**, 118 (1987).
[37] D. M. Greenberger, M. A. Horne, and A. Zeilinger, Phys. Today **46**(8), 22 (1993).
[38] A. Zeilinger, Am. J. Phys. **49**, 882 (1981).
[39] P. Elias, Ann. Math. Stat. **43**, 865 (1972).
[40] Y. Peres, Ann. Stat. **20**, 590 (1992); http://www.jstor.org/stable/2242181
[41] M. Dichtl, in *Fast Software Encryption*, Lecture Notes in Computer Science Vol. 4593, edited by A. Biryukov (Springer, Berlin, 2007), pp. 137–152.
[42] P. Lacharme, in *Fast Software Encryption*, Lecture Notes in Computer Science Vol. 5086, edited by K. Nyberg (Springer, Berlin, 2008), pp. 334–342.
[43] K. Svozil, New J. Phys. **8**, 39 (2006); J. Phys. A **38**, 5781 (2005).
[44] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998).
[45] T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, N. Langford, T. Jennewein, and A. Zeilinger, e-print arXiv:0811.3129.
[46] V. Jacques, E. Wu, F. Grosshans, F. Treussart, P. Grangier, A. Aspect, and J.-F. Roch, Science **315**, 966 (2007).
[47] A. Peres, Am. J. Phys. **46**, 745 (1978).