Quantum Random Number Generators

http://tph.tuwien.ac.at/∼svozil/publ/2017-Svozil-Shaping the future Quantum Technology Flagship - WS, 18.1.2017-pres.pdf
DOI: 10.3354/esep00171, arXiv:1605.08569

Karl Svozil

ITP/Vienna University of Technology, Austria
& CS/University of Auckland, NZ
svozil@tuwien.ac.at

Vienna, January 18th, 2017

Early QRNGs using quantum complementarity

- Quantum coin toss: prepare in a (pure) state, measure in another (non-orthogonal) direction [KS, 1990, DOI: 10.1016/0375-9601(90)90408-G; ...]
- Realizations by various groups (eg, Jennewein, Zeilinger et al, 2000, DOI: 10.1063/1.1150518; Stefanov, Gisin et al., 2000, DOI: 10.1080/09500340014790 8; Fürst, Weinfurter et al, 2010, DOI: 10.1364/OE.18.013029; Quantis TRNG (True Random Number Generator) - ID Quantique, 2000–2017; ...)
- Potential problem: complementarity has classical models; no guarantee for value indefiniteness (eg, KS, 2009, DOI: 10.1016/B978-0-444-52869-8.50015-3)

QRNG featuring quantum value indefiniteness

- Quantum value indefiniteness in higher dimensional ($D \geq 3$) systems; no classical *double* (eg, Pitowski, 1998, DOI:10.1063/1.532334; KS, 20109, DOI: 10.1103/PhysRevA.79.054306; Abbot et al, 2012-2015, DOI: 10.1103/PhysRevA.86.062109, 10.1103/PhysRevA.89.032109, 10.1063/1.4931658; ...);
- Realizations by various groups (eg, Hai-Qiang et al, 2004, DOI: 10.1088/0256-307X/21/10/027; Pironio et al., 2010, DOI: 10.1038/nature09008; ...)
- Challenge: dim-3 (qtrits); GHZ-type realization (strict nonstochastic violation of classical predictions).

Questions and challenges

- Normalization of bias of (non)independent events (eg, von Neumann, 1951, Various Techniques Used in Connection With Random Digits; ...)
- Where exactly is the randomness located/grounded? Beam splitters are unitary (one-to-one) elements; nesting argument of Everett DOI: 10.1103/RevModPhys.29.454 & Wigner DOI: 10.1007/978-3-642-78374-6_20
- Claims of absolute and irreducible randomness are provable unprovable (by reduction to the recursive unsolvability of the halting and the rule inference problem).

General questions and challenges

- What is the particular source of quantum speedups (eg, entanglement, coherence=parallelism, partitioning of information)?
- How to cope with man-in-the middle attacks on quantum cryptography? How much authentification is needed for key growing? Claims of "absolute security" wrt qc; Specker's "Jesuit lies"
- Where is a "killer-app" in the zoo of qantum algorithms http://math.nist.gov/quantum/zoo/ ?
- Ethics and certification issues related to science marketing; in particular the "quantum mechanis is magic/hocus pocus/abracadabra" tour: KS, Ethics in Science and Environmental Politics (ESEP), DOI: 10.3354/esep00171, arXiv:1605.08569

Thank you for your attention!