# Private random number generation through remote atom entanglement

S. Olmschenk[1],* S. Pironio[2,3], A. Acin[4,5], S. Massar[2], A. Boyer de la Giroday[6], D. N. Matsukevich[1], P. Maunz[1], D. Hayes[1], L. Luo[1], T. A. Manning[1], and C. Monroe[1]
[1] *Joint Quantum Institute, National Institute of Standards and Technology and University of Maryland Department of Physics, Gaithersburg, MD 20899, USA*
[2] *Laboratoire d'Information Quantique, CP 225, Université Libre de Bruxelles, Bvd Du Triomphe, 1050 Bruxelles, Belgium*
[3] *Group of Applied Physics, University of Geneva, 1211 Geneva, Switzerland*
[4] *ICFO-Institut de Ciencies Fotoniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain*
[5] *ICREA-Institucio Catalana de Recerca i Estudis Avancats, 08010 Barcelona, Spain*
[6] *Cavendish Laboratory, Cambridge University, Cambridge CB3 0HE, UK*

Random number generation is vital for a wide range of applications, including numerical simulation, gambling, and cryptography. However, verifying the randomness of a bit stream generated by a device is exceedingly difficult. Even if a sequence of numbers passes all of the standard statistical tests, it is often impossible to certify the authenticity of the device and rule out the possibility that an adversary has loaded a predetermined sequence into an internal memory. Recently, it has been shown that the non-local correlations between entangled quantum systems can be used to verify the generation of true random numbers [1, 2]. This insight enables the construction of a private random number generator whose output can be verified as random through the violation of a Bell inequality, without requiring any assumptions about the internal mechanisms of the device.

We demonstrate the operation of a private random number generator using two entangled ytterbium ions separated by a distance of about one meter [1]. The quantum bit (qubit) in each atom is encoded in the magnetic-field-insensitive "clock" states of the $^2S_{1/2}$ level, $|0\rangle \equiv |F=0, m_F=0\rangle$ and $|1\rangle \equiv |F=1, m_F=0\rangle$. At the beginning of every attempt to establish entanglement between the two distant atomic qubits, each atom is initialized to the state $|0\rangle$ by 1 $\mu$s of optical pumping [3] (Fig. 1(a)). Microwave radiation with independently controlled phase and duration at each atom is then applied to prepare both atoms in state $(|0\rangle + |1\rangle)/\sqrt{2}$ (Fig. 1(b)). Next, a $\pi$-polarized picosecond pulse of light near 370 nm coherently drives the ground state populations to complementary states in the $^2P_{1/2}$ excited state, as illustrated in Fig. 1(c). Each atom then spontaneously decays while emitting a single photon. Considering only $\pi$-decays (filtering out $\sigma$-decays using polarizers) results in the frequency of the emitted photon being entangled with the atomic qubit (Fig. 1(d)). Entanglement between the two distant atoms is accomplished through the interference and coincident detection of these spontaneously emitted photons [4, 5]. After every atomic entanglement event, the

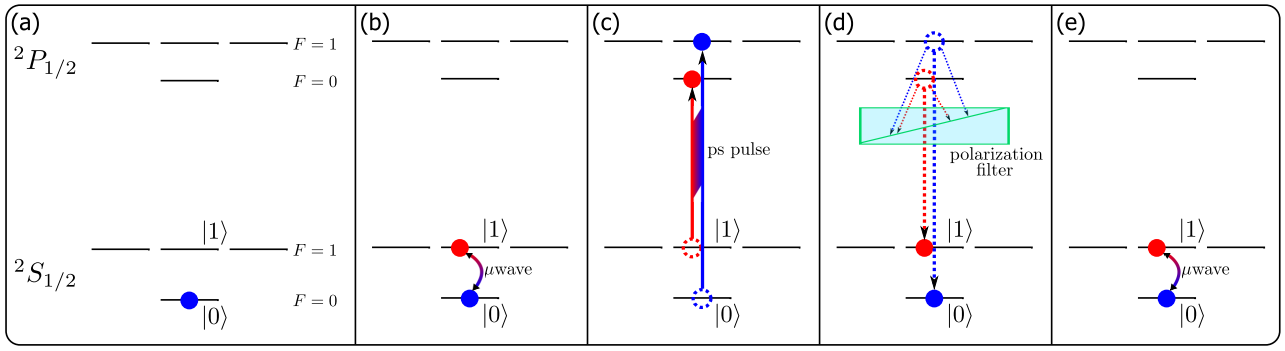


FIG. 1: (a) After optical pumping, each atom has been initialized to the state $|0\rangle$. (b) A microwave pulse with independently controlled phase and duration at each atom prepares both atoms in the $(|0\rangle + |1\rangle)/\sqrt{2}$ state. (c) A picosecond pulse of light near 370 nm coherently drives population from the ground state to the excited state. Here, atomic selection rules prevent mixing of the populations. (d) The atom spontaneously decays while emitting a single photon. If only $\pi$-decays are detected ($\sigma$-decay are blocked from reaching the detectors by polarization filters) then the frequency of the emitted photon is entangled with the atomic qubit. (e) Measurement of the atomic qubit in any basis may be acheived by applying a microwave rotation prior to fluorescence detection.

*Electronic address: steven.olmschenk@gmail.com

 

measurement basis for each atom is randomly assigned one of two values that allows for observation of a CHSH Bell inequality violation [6, 7], and is set by coherent microwave rotations prior to readout. The atoms are measured using standard fluorescence techniques with a detection fidelity greater than 97% [3] and perfect efficiency (every event is recorded). The atomic measurement results constitute the output of the random number generator.

The CHSH Bell inequality observable [6] is estimated by the accumulation of 3016 entanglement events, resulting in $S = 2.414 \pm 0.058 > 2$ [1]. The violation of the CHSH inequality allows us to place a lower bound on the entropy of the recorded bit stream. The observed $S$ value guarantees that 42 private random numbers are generated at a 99% confidence level, irrespective of any detailed assumptions of the device.

The efficiency of the random number generator is limited in the current setup by the low success probability ($2\times10^{-8}$) of the heralded entanglement operation. To improve this, effort is now focused on increasing the photon collection efficiency by incorporating high numerical aperture optics near the atoms, or coupling the light emitted by the atoms to an optical cavity. Advances towards this end may also enable a quantum repeater architecture for long-distance quantum communication, and the generation of large-scale entanglement for universal quantum computation [8].


[1] S. Pironio et al., "Random numbers certified by Bell's theorem", *Nature* **464**, 1021 (2010).

[2] R. Colbeck, *Quantum and Relativistic Protocols for Secure Multi-Party Computation*, PhD thesis, Univ. Cambridge, 2007.

[3] S. Olmschenk et al., "Manipulation and Detection of a Trapped $Yb^+$ Hyperfine Qubit", *Phys. Rev. A* **76**, 052314 (2007).

[4] C. Simon and W. T. M. Irvine, "Robust Long-Distance Entanglement and a Loophole-Free Bell Test with Ions and Photons", *Phys. Rev. Lett.* **91**, 110405 (2003).

[5] L.-M. Duan et al., "Probabilistic quantum gates between remote atoms through interference of optical frequency qubits", *Phys. Rev. A* **73**, 062324 (2006).

[6] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed Experiment to Test Local Hidden-Variable Theories", *Phys. Rev. Lett.* **23**, 880 (1969).

[7] D. N. Matsukevich, P. Maunz, D. L. Moehring, S. Olmschenk, and C. Monroe, "Bell Inequality Violation with Two Remote Atomic Qubits", *Phys. Rev. Lett.* **100**, 150404 (2008).

[8] L.-M. Duan and C. Monroe, "Colloquium: Quantum networks with trapped ions", *Rev. Mod. Phys.* **82**, 1209 (2010).


 