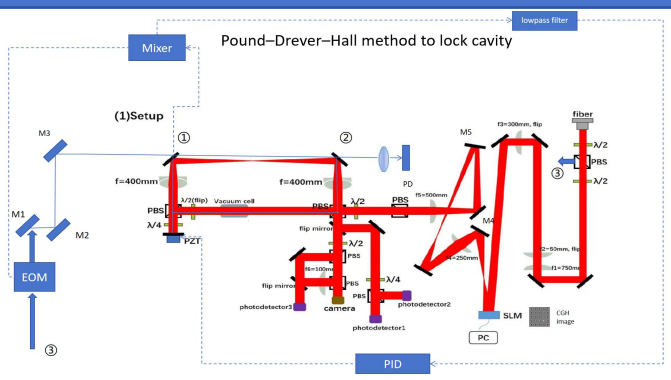
Stable random number generation in a PSR-based DOPO cavity

Zhiren Zhang [1], Dongdong Hao[1], K. S. Manannikov[2], Yanhong Xiao[1]
[1]Fudan University, [2]Weizmann Institute of Science, Israel

Introduction

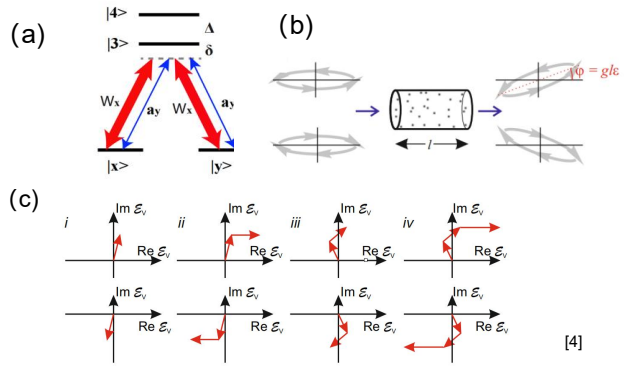
- Random numbers based on quantum origins possess unpredictability and infinite periodicity, achieving information-theoretic absolute security.
- Traditional methods using photon vacuum fluctuations[1] and laser phase fluctuations[2] suffer from poor entropy source randomness, requiring extensive post-processing. Meanwhile, random number generation based on fiber DOPO systems[3] is limited by cavity linewidth and long lifetime of photons , resulting in low generation rate.
- In DOPO system based on the warm atomic vapor cell , quantum random numbers based on polarization self-rotation and cavity mode selection exhibit robustness against fluctuations in laser intensity and frequency detuning. Furthermore, coherence caused by atomic flight helps narrow the linewidth and can enhance the random number generation rate.
- With the aid of machine learning, long-term stable unbiased randomness is achieved, passing all NIST tests with only weak post-processing.
- Additionally, the sensitivity of randomness to magnetic fields near the unbiased point holds promise for applications in precision measurement and multi-parameter sensing.

Setup



- Generating a spatial light array using a SLM
- The 4F system is designed to match the light pattern with Rb^{87} vapour cell .
- Bistability achieved by PSR-based DOPO in the cavity.

Theory Ⅰ: Master equation of four-wave mixing in dissipative system



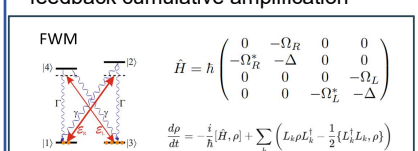
[4]

$$\begin{pmatrix} \mathcal{E}_H \\ \mathcal{E}_V^{(n+1)} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{\eta}e^{i\psi} \end{pmatrix} \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix} \begin{pmatrix} \mathcal{E}_H \\ \mathcal{E}_V^{(n)} \end{pmatrix} + \begin{pmatrix} \mathcal{E}_H \\ 0 \end{pmatrix}$$

$$E_V^{(n+1)} = \sqrt{\eta}e^{i\psi}\left(E_V^{(n)} + gl\,ImE_V^{(n)}\right)$$

Fig: (a)Energy level diagram of four-wave mixing.(b)Polarized self-rotation.(c)Bistability.

Vertically polarized light: Vacuum fluctuation → random selection of rotation direction → PSR induced change in polarization → cavity feedback cumulative amplification



$$\hat{H} = \hbar \begin{pmatrix} 0 & -\Omega_R & 0 & 0 \\ -\Omega_R^* & -\Delta & 0 & 0 \\ 0 & 0 & 0 & -\Omega_L \\ 0 & 0 & -\Omega_L^* & -\Delta \end{pmatrix}$$

$$\frac{d\rho}{dt} = -\frac{i}{\hbar}[\hat{H},\rho] + \sum_k \left(L_k \rho L_k^\dagger - \frac{1}{2}\{L_k^\dagger L_k, \rho\}\right)$$

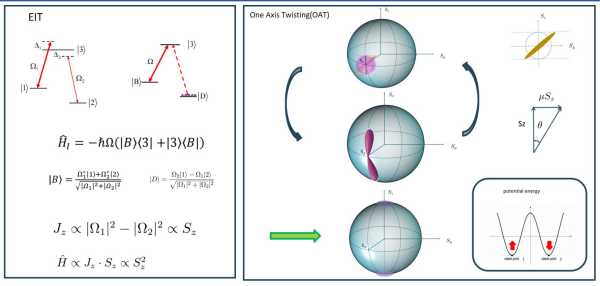
$$\chi_{R,L} = N\mathrm{Tr}\hat{\rho}\hat{d}_{R,L} \qquad n_{R,L} - 1 \approx \frac{1}{2}\chi_{R,L}$$

$$\begin{aligned}
\dot{\rho}_{11} &= \Gamma\rho_{44} + \gamma\rho_{22} + i\Omega_R\rho_{12}^* - i\Omega_R^*\rho_{12} \overset{!}{=} 0;\\
\dot{\rho}_{22} &= -\Gamma\rho_{22} - \gamma\rho_{22} - i\Omega_R\rho_{12}^* + i\Omega_R^*\rho_{12} \overset{!}{=} 0;\\
\dot{\rho}_{33} &= \Gamma\rho_{22} + \gamma\rho_{44} + i\Omega_L\rho_{34}^* - i\Omega_L^*\rho_{34} \overset{!}{=} 0;\\
\dot{\rho}_{44} &= -\Gamma\rho_{44} - \gamma\rho_{44} - i\Omega_L\rho_{34}^* + i\Omega_L^*\rho_{34} \overset{!}{=} 0;\\
\dot{\rho}_{12} &= -\left(\frac{\gamma+\Gamma}{2} + i\Delta\right)\rho_{12} - i\Omega_R(\rho_{11} - \rho_{22}) \overset{!}{=} 0;\\
\dot{\rho}_{34} &= -\left(\frac{\gamma+\Gamma}{2} + i\Delta\right)\rho_{34} - i\Omega_L(\rho_{33} - \rho_{44}) \overset{!}{=} 0;\\
\dot{\rho}_{24} &= -\Omega_R^*\rho_{14} - \Omega_L\rho_{23}^* \overset{!}{=} 0;\\
\dot{\rho}_{23} &= i\Delta\rho_{23} + \Omega_R^*\rho_{13} - \Omega_L^*\rho_{24} \overset{!}{=} 0;\\
\dot{\rho}_{14} &= -i\Delta\rho_{14} + \Omega_R\rho_{24} - \Omega_L\rho_{13}^* \overset{!}{=} 0;\\
\dot{\rho}_{13} &= -\Omega_R\rho_{23} - \Omega_L^*\rho_{14} \overset{!}{=} 0
\end{aligned}$$

$$\varphi(\varepsilon) = -\frac{1}{2}kl(n_R - n_L) \sim \frac{\delta\sin(2\varepsilon)}{(2+8\delta^2)+I/I_{\mathrm{sat}}+\cos(4\varepsilon)I/I_{\mathrm{sat}}} \longrightarrow \boxed{\varphi \approx gl\varepsilon}$$

1. $\psi(\epsilon)$ is odd in $\epsilon \to (E_H, E_V)$ with $-\epsilon$ is also a steady state.
2. Odd self-rotation angle: $-\epsilon$ yields another steady-state solution (E_H, E_V^*).
3. Steady states come in (ϵ) and $(-\epsilon)$ pairs due to odd $\psi(\epsilon)$.

Theory Ⅱ: Evolutionary dynamics of bistability from the perspective of the Poincaré sphere



$$\hat{H}_I = -\hbar\Omega(|B\rangle\langle 3| + |3\rangle\langle B|)$$

$$|B\rangle = \frac{\Omega_1^*|1\rangle + \Omega_2^*|2\rangle}{\sqrt{|\Omega_1|^2+|\Omega_2|^2}} \qquad |D\rangle = \frac{\Omega_2|1\rangle - \Omega_1|2\rangle}{\sqrt{|\Omega_1|^2+|\Omega_2|^2}}$$

$$J_z \propto |\Omega_1|^2 - |\Omega_2|^2 \propto S_z$$

$$\hat{H} \propto J_z \cdot S_z \propto S_z^2$$

Experimental Results

1.Machine learning-assisted long-term stable randomness

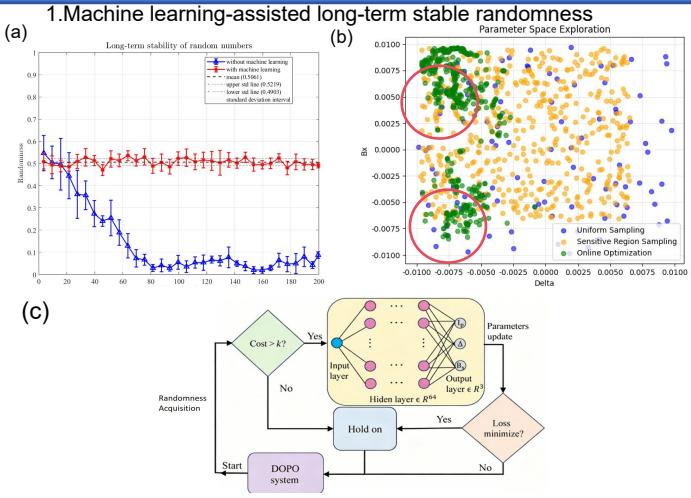


Fig: (a) Machine learning has stabilized the randomness.(b)The exploration of the parameter space has converged.(c)Flowchart of real-time feedback-based machine learning for suppressing system drift.

2.After weak post-processing, the bit sequence passed the NIST test

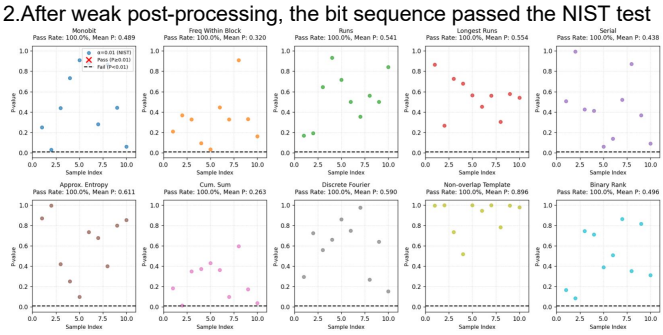


Fig: For each module, if the proportion of p-values higher than 0.01 reaches over 95%, it is considered to have passed NIST test.

3.The sensitivity of the parameters around the randomness of 0.5 is expected to be applied to precise measurements

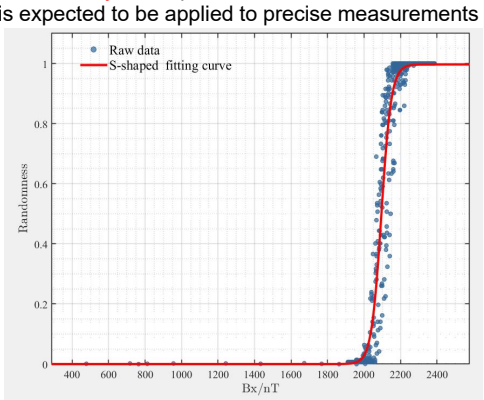


Fig:The randomness is sensitive to the measured magnetic field. Dynamic range is 68 nT.

$$\text{Minimum detectable signal:}\delta B = \frac{noise}{slope} = \frac{\Delta\omega}{\partial\omega/\partial B}$$

Conclusion

- PSR-based DOPO in warm atomic system → single random bit via bistability
- Machine learning-based online feedback dynamically compensates symmetry breaking from system parameter drift, realizing a stable, interference-immune entropy source.
- After post-processing, the RN sequence satisfies the NIST statistical tests.
- Sensitivity of randomness: expected to be used in Magnetic field tracking and magnetometers.

References: [1]Gabriel, Christian, et al. Nature Photonics 4.10 (2010): 711-715. [2]Xu F, Qi B, Ma X, et al. Optics express, 2012, 20(11): 12366-12377. [3]Quinn L, Xu G, Xu Y, et al. Optics Letters, 2023, 48(14): 3741-3744. [4]Manannikov K S, Mironova E I, Poliakov A S, et al. Optics Letters, 2025, 50(3): 792-795.