

Study of atmospheric turbulence with applications in cryptography

Advisor: J Solomon Ivan, Department of Physics, Email: solomonivan@iist.ac.in

Keywords: Phase estimation, phase-unwrapping, interferometry, signal processing, hardware interface, programming

Description:

Recently atmospheric turbulence has been explored for its possible application in cryptography that include random number generation and secret key distillation. Some work has already been initiated at IIST in this regard. The proposed work would involve setting up an optical test facility to conduct experimental work with applications in cryptography. This includes estimation of random phases introduced by atmospheric turbulence in real time. Prerequisites include strong background in classical optics with good knowledge in signal processing. Hardware interfacing and programming skills are preferable. Candidates with Ph.D in physics with optics/holography background, and Ph.D in signal/image processing from department of electrical/electrical and communication engineering may apply.

References:

C. F. Bas, N. C. Donnangelo, M. D. Drake, D. Gervais, J. J. Rushanan, "Generating identical numerical sequences utilizing a physical property and secure communication using such sequences," US Patent 8,189,785, May 29, (2012).

M. D. Drake, C. F. Bas, D. Gervais, P. F. Renda, D. Townsend, J. J. Rushanan, J. Francoeur, N. Donnangelo, and M. D. Stenner, "Optical key distribution system using atmospheric turbulence as the randomness generating function: classical optical protocol for information assurance," *Opt. Engg.* **52**, 055008–055008 (2013).

D. G. Marangon, G. Vallone, and P. Villoresi, "Random bits, true and unbiased, from atmospheric turbulence," arXiv:1309.4114.