Secure Communication with Coded Wavefronts

***Ravitej Uppu*[1], *Tom A. W. Wolterink*[1,2], *Sebastianus A. Goorden*[1], *Boris Škorić* [3], *Allard P. Mosk*[1,4], *and Pepijn W. H. Pinkse*[1]**

1. Complex Photonic Systems (COPS), MESA+ Institute for Nanotechnology, University of Twente, P.O. Box 217, 7500 AE Enschede, The Netherlands

2. Laser Physics and Nonlinear Optics (LPNO), MESA+ Institute for Nanotechnology, University of Twente, P.O. Box 217, 7500 AE Enschede, The Netherlands

3. Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands

4. Nanophotonics, Debye Institute for Nanomaterials Science, Center for Extreme Matter and Emergent Phenomena, Utrecht University, P.O. Box 80.000, 3508 TA Utrecht, The Netherlands

Communication between a sender and receiver can be made secure by encrypting the message using public or private shared keys. Quantum key distribution utilizes the unclonability of a quantum state to securely generate a key between the two parties [1]. However, without some way of authentication of either the sender or the receiver, a man-in-the-middle attack with an eavesdropper mimicking the receiver can break the security of the protocol.

Here, we discuss securing communication schemes against the man-in-the-middle attacks through the use of an optical Physical Unclonable Function (PUF). Light propagation through opaque scattering media, such as white paint and teeth, gives rise to a complex interference pattern, called speckle. The high sensitivity of the speckle pattern to the exact position and the size of the millions of nanoscopic scatterers within the medium led to its applicability as a physical unclonable function [2]. This sensitivity has recently been exploited for quantum-secure authentication [3,4] and it has been suggested to incorporate PUFs in quantum key distribution for authentication purposes [3,5].

We create and utilize wavefronts that can be efficiently decoded only by transforming them with the PUF. Several methods to achieve this will be discussed and preliminary communication experiments with complex wavefronts will be shown. The proposed schemes strengthen the emerging applicability of opaque scattering media in quantum security and information processing [6].

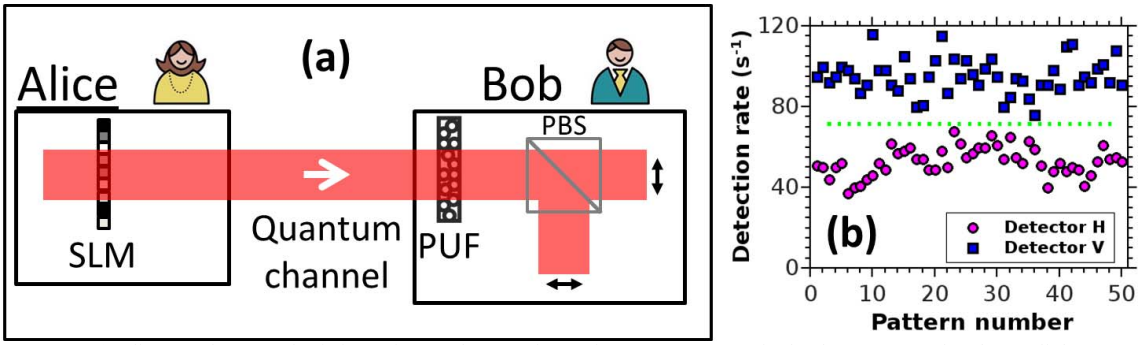

Fig. 1 (a) Alice (sender) encodes information on the wavefront of a quantum state (single photons or weak coherent light) using a spatial light modulator (SLM) which can be decoded only using the PUF possessed by Bob (receiver). (b) Measured photodetections showing clear contrast in horizontal (H; magenta circles) and vertical (V; blue squares) polarization channels when 50 different wavefronts corresponding to V were sent.

References

[1] M. Peev et al., "The SECOQC quantum key distribution network in Vienna," New J. Phys. **11**, 075001 (2009).
[2] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," Science **297**, 2026-2030 (2002).
[3] S. A. Goorden, M. Horstmann, A. P. Mosk, B. Škorić, and P. W. H. Pinkse, "Quantum-secure authentication of a physical unclonable key," Optica **1**, 421-424 (2014).
[4] B. Škorić, P. W. H. Pinkse, and A. P. Mosk, "Authenticated communication from Quantum Readout of PUFs," Cryptology ePrint Archive, ia.cr/2016/971 (2016).
[5] B. Škorić, "Quantum Readout of Physical Unclonable Functions," Int. J. Q. Inf. **10**, 1250001 (2012).
[6] P. W. H. Pinkse and A. P. Mosk, "Multiple-scattering materials as physical unclonable functions," pp.32-33 in B. Javidi et al., "Roadmap on optical security," J. Opt. 18, 083001 (2016).