Abstract:

The field of disordered photonics has grown immensely over the past two decades, ranging from investigations into fundamental topics such as Anderson localization and anomalous transport, to applications in imaging, random lasing and solar energy [1]. In this talk I will discuss another promising application that realize cryptography and security by random, disordered, and unclonable physical structures. Optical physical unclonable functions (O-PUFs) are cryptographic primitives made of any disordered/scattering/complex physical objects, that for a given input and conditions, provides a defined "digital fingerprint" output that serves as a unique identifier [2]. The main idea is to exploit the unique physical variations which occur naturally during device manufacturing, or the intrinsic complexity of any natural system to generate cryptographic keys. O-PUFs solve the problem of cyber-attacks in non-volatile memories by an on-demand/on-the-fly cryptographic key generation, and can, in principle, overcome the limitations of conventional digital security enabling cryptographic protocols immune against attacks by future quantum computers [3]. O-PUF constitute an exceptionally promising tool for new forms of cost-effective, secure, and scalable networks. I will present our latest results in this field, covering fundamental aspects of photonics and information theory [4], the practical aspect of the unclonability [5], the realization of anticonterfeiting tokens [6] and the realization of a multilevel O-PUF by exploiting reconfigurable light responsive photonic materials [7]. Finally, I will discuss the possibility to use the multilevel O-PUF for nonlinear [8] and quantum read-out cryptography [9].