Abstract:

One of Alan Turing's most influential papers is his 1950 Computing machinery and intelligence, in which he introduces the famous "Turing test" for probing the nature of intelligence by evaluating the abilities of machines to behave as humans. In this test, which he calls the "Imitation Game," a (human) referee has to distinguish between two (remote and separate) entities, a human and a computer, only by observing answers to a sequence of arbitrary questions to each entity. This lecture will exposit, through examples from a surprisingly diverse array of settings, the remarkable power of this basic idea to understand many other concepts. I will discuss variations of the Imitation Game in which we change the nature of the referee, and of the objects to be distinguished, to yield different analogs of the Turing test. These new Imitation Games lead to novel, precise, and operative definitions of classical notions, including secret, knowledge, privacy, randomness, proof, fairness, and others. These definitions have in turn led to numerous results, applications, and understanding. Some, among many consequences of this fundamental paradigm, are the foundations of cryptography, the surprising discoveries on the power and limits of randomness, the recent influential notion of differential privacy, and breakthrough results on patterns in the prime numbers and navigation in networks. Central to each of these settings are computational and information theoretic limitations placed on the referee in the relevant Imitation Game. This lecture will survey some of these developments. It assumes no specific background knowledge.