Research Proposal: On Quantum Cryptography Primitives

13th July 2016

The broad goal of the research would be to construct techniques for quantifying advantages of and performing cryptography using quantum physics. Quantum physics has peculiar properties which distinguishes it from behaviour of macroscopic objects. Bell was among the first to describe a physical situation which classical physics can not explain, unless we allow super luminal (faster than light) communication. Entanglement is a property of a quantum system which is necessary for the aforesaid result to hold, which has been experimentally verified. Consequently, entanglement has been studied as a resource and has been applied to quantum cryptography, specifically to quantum key distribution. The use of Bell's inequality, as they are called, to quantify communication complexity has been explored. The relation between non-locality and cryptography, therefore, is of key interest and will be explored further in this project. Further, a more general notion, that of contextuality, has been introduced as a tool to study cryptography only recently. One possible direction could be extension of known quantum algorithms for cryptography which rely on entanglement, to achieve higher robustness and ease of implementation, using contextuality as a resource.

Continuous variable quantum computing has been gaining momentum lately. Cryptographic applications of the same are of particular interest. Recent work on successful extension of Bell's inequality to using continuous spectrum observables might prove useful to this effect. Typical cryptography protocols discretise time which is in stark contrast with physical systems which evolve under a Hamiltonian with time as a continuous parameter. This paradigm is expected to prove itself to be a useful tool for advancing cryptographic primitives. Quantum Information Complexity will perhaps serve as a second such tool for the aforesaid purpose. Here complexity is quantified using Shannon's notion of information. The difficulty of course is that this is a classical notion and when extended to quantum physics, the definition ceases to be unique. It is felt that using the framework of continuous time protocols an appropriate definition can be arrived at.

An immediate and specific goal of this project would be to construct a quantum algorithm for a known cryptography primitive, a distrustful coin toss: the problem of sharing the outcome of an unbiased coin, among two physically separated distrustful players. This problem is of particular interest because classically, no unconditionally secure protocol exists, viz. a player with unbounded computational power can always bias the results. However, using the magic of mathematical analysis, it was proven in 2007, that an unconditionally secure protocol exists within the purview of quantum mechanics. As a remark I might state that Dr J. Roland (who has agreed to supervise my work), has given an alternate proof to a related problem. The issue with the proof of the aforesaid is that it is non-constructive and therefore yields no hints into solving this problem. This has consequently been an open problem for 9 years but due to various preliminary results obtained by Dr J. Roland and his team, this specific problem will hopefully get solved as a part of this research project.