Title:	Studies of quantum contextuality, Bell non-locality and their role in quantum key distribution protocols
Authors:	Nirankari, Jaskaran Singh
Keywords:	Quantum contextuality Bell non-locality Protocols
Issue Date:	28-Jul-2021
Publisher:	IISERM
Abstract:	This thesis deals with foundational concepts of quantum theory including contextuality and Bell non-locality, and their applications in quantum key dis- tribution (QKD) protocols. We provide a generalization of the standard notion of quantum contextuality and show that it encompasses a broader range of scenarios which can be deemed (non-)contextual. This generalization is then used to depict a violation of a new non-contextual inequality developed by us. The violation so exhibited can be achieved by a single measurement device, which implements a positive operator valued measure (POVM). This number is significantly smaller than the current contextual scenarios and is optimal as no further reductions are possible. The new NC inequalities so developed can be easily generalised further for n-cycle scenarios and any number of sequential measurements. We then develop a QKD protocol which is based on the principle of con- textuality monogamy and show that it is unconditionally secure for individual attacks by an eavesdropper. We use the KCBS scenario to share a secure key among two parties via a prepare and measure QKD scheme. Our protocol does not require the use of entanglement, which is a costly resource to produce, while also allowing a security check via a NC inequality like in the case of Bell inequal- ities. This is achieved by the principle of contextuality monogamy which forbids an eavesdropper to attain information about the secure key without disturbing the correlations among the parties. We then apply the same strategy to entropic NC inequalities to show that they can also be used to perform secure QKD. We show when a entropic NC scenario can have a monogamous relationship and how it can be derived using a graph theoretic approach. We apply the principle of monogamy along similar lines as before to show that a device independent security proof of the the protocol is possible. This is unlike the previous approach. We then analyse the role of Bell-CHSH inequality in entanglement based QKD. More specifically, we show that violation of Bell-CHSH is not a sufficient criteria for security, while it is a necessary one. We construct a geometrical representation of correlations for two qubits from which it is quite easy to infer the usefulness of various states for QKD. We also analyse the role of local filtering in QKD. States which do not violate the Bell-CHSH inequality can be made useful for QKD after local filtering. However, not all states can be made useful including useless Bell diagonal states. We finally analyse quantum contextuality in pre- and post-selection scenarios 1which have gained a lot of traction in recent years. Statistics of various outcomes in these scenarios is determined by the ABL rule. We show that this rule is non-contextual in non-paradoxical situations, thereby indicating that it does not entirely capture the essence of quantum theory. We further show that by removing post-selection, it is possible to achieve the maximum violation of KCBS inequality as dictated by quantum theory. This indicates that post- selection is a root cause for paradoxical situations.
URI:	http://hdl.handle.net/123456789/3754
Appears in Collections:	MP-13

Files in This Item:

File	Description	Size	Format	
thesis.pdf		3.92 MB	Adobe PDF	View/Open