Quantum conferencing based on Mermin's contextuality inequality

Rajni Bala, Sooryansh Asthana & V. Ravishankar

Indian Institute of Technology Delhi, New Delhi, India.

Abstract

Quantum key distribution (QKD) is one of the first application of quantum physics which has entered the commercial market. The security of QKD protocols relies on the quantum nature of the physical system used. In this work, we present a quantum conferencing protocol, security of which depends upon the contextuality of single qudit system. Thus, our protocol come under the prepare and measure scheme. It has been shown[1] that nonlocality inequalities probes contextuality in single qudit system of suitable dimensions. We use this result and for the purpose of pedagogy, show that with appropriate mapping Mermin's nonlocality inequality[2] detects contextuality in a single qudit system of suitable dimensions. In the proposed protocol, Mermin's contextuality inequality act as a security check. Unlike the non-locality based protocol, this protocol does not involve entangled states, whose generation is very difficult. The proposed protocol can be implemented without any compromise in the key generation rate in certain noisy channels. The experimental key generation rate of the protocol will also be high if one uses weak coherent pulses instead of the limited brightness of entangled photon pair sources. With the advancement in generation and manipulation of higher dimensional orbital angular momentum(OAM) states of light[3,4], our protocol can be realised experimentally.

Mapping from $\mathcal{H}^{2^{\otimes N}} \rightarrow \mathcal{H}^{2^N}$

- Let $\mathfrak{B}_1$ and $\mathfrak{B}_2$ be the basis for N-qubit and 2^N dimensional qudit system.

$$\mathfrak{B}_1 \equiv \{|j_1 j_2 \cdots j_N\rangle; j_k \in \{0,1\}, 1 \leq k \leq N\}; \quad \text{and } \mathfrak{B}_2 \equiv \{|0\rangle, |1\rangle, \cdots, |\mathrm{D}-1\rangle\}. \tag{1}$$

- The bijective mapping between the two basis is defined as $|j_1 \cdots j_N\rangle \leftrightarrow \left|\sum_{k=1}^{N} 2^{N-k} j_k\right\rangle = |j\rangle$.
- The symbols X_k, Y_k, Z_k shall be reserved for the Pauli matrices acting over the space of the k^{th} qubit. The corresponding observables acting on a single qudit system will be represented by $\mathbb{X}_k, \mathbb{Y}_k, \mathbb{Z}_k$.
- The unitary transformations performed by the k^{th} party in a multi-party system, represented by U_k, are mapped to $\mathbb{U}_k$ in a single qudit, i.e.,$\mathbb{1}^{\otimes k-1} \otimes U_k \otimes \mathbb{1}^{\otimes N-k} \leftrightarrow \mathbb{U}_k$. The unitary transformations performed on the combined space of j^{th} and k^{th} party, represented by U_{jk}, are mapped to $\mathbb{U}_{jk}$ in a single qudit system. Similarly, the transformation acting on the combined space of first k parties of a multiparty system, $U_{1\cdots k}$, is mapped to $\mathbb{U}_{1\cdots k}$ in a single qudit system straightforwardly.

Mermin nonlocality as contextuality inequality in 2^N-level system

Mermin's nonlocality inequality[2] also detect contextuality in single qudit system of appropriate dimensions[1].Equivalent Mermin inequality is:

$$\mathbb{M}_N = \frac{1}{2i}\left|\left\langle \prod_{k=1}^{N}(\mathbb{X}_k + i\mathbb{Y}_k) - \prod_{k=1}^{N}(\mathbb{X}_k - i\mathbb{Y}_k)\right\rangle\right| \leq c, \quad c = 2^{N/2} \text{ for even N}, \quad c = 2^{\frac{N-1}{2}} \text{ for odd N}. \tag{2}$$

which gets maximally violated by the state $|\Psi_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|2^N - 1\rangle)$. Consider the following two contexts:

Context 1 ($\mathbb{Z}_1\mathbb{Z}_2\cdots\mathbb{Z}_{N-1}\mathbb{Z}_N$): Suppose the outcome of $\mathbb{Z}_1$ is $+1(-1)$. Then, the outcomes of observables $\mathbb{Z}_2, \mathbb{Z}_3, \cdots, \mathbb{Z}_N$ will be $+1(-1)$ with unit probability.
Context 2 ($\mathbb{Y}_1\mathbb{Z}_2\cdots\mathbb{Z}_N$): Let the outcome of the measurement of $\mathbb{Y}_1$ be once again, $+1$. Following it, the measurement of observable $\mathbb{Z}_2$ will yield $+1$ or -1 with equal probability. Thereafter, the measurement of $\mathbb{Z}_3, \cdots, \mathbb{Z}_N$ will definitely yield $+1$. Thus, the outcome of $\mathbb{Z}_2$ depends on the set of commuting observables it is measured with, i.e., it depends on the *context*.
Thus, Mermin's inequality probes contextuality in a qudit of appropriate higher dimension and can be referred to as Mermin's contextuality inequality.

Advantages

- Above protocol does not employ entangled states and can be implemented using higher dimensional orbital angular momentum(OAM) states of light[3,4].
- The experimental key generation rate will be higher as compared to entangled one because weak photon pulses can be used as compared to limited brightness of entangled photon pair sources.

Rajni Bala and Sooryansh Asthana thank UGC and CSIR respectively for financial support.

Quantum conferencing based on Mermin's contextual inequality

1. All the observables are publicly announced.
2. Let $|\Psi_M\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|2^N - 1\rangle)$ be the reference state. Bob_1 randomly prepares his system in the state $|\Psi'_M\rangle = \mathbb{U}_1\Pi^{\mathbb{O}}_0|\Psi_M\rangle$, $\mathbb{O} \in \{\mathbb{X}_1, \mathbb{Y}_1, \mathbb{Z}_1\}$ with equal probability and sends it to Bob_2.
3. Bob_2 randomly measures any one of the observables $\mathbb{X}_2, \mathbb{Y}_2, \mathbb{Z}_2$. After making measurements on the state, he performs arbitrary transformation $\mathbb{U}_{12}$. Thereafter, he sends the transformed state to Bob_3.
4. This process will continue till Bob_N performs his measurement. This concludes the first round. This procedure is repeated for many rounds.
5. After many such rounds are completed, the choices of observables are revealed for each round. The outcomes of such rounds, in which all the N-Bobs choose their respective observable from the set $\{\mathbb{Z}_1, \mathbb{Z}_2, \cdots, \mathbb{Z}_N\}$, are not revealed.
6. The outcomes of rounds, in which all the N-Bobs choose their respective observable from the set $\{(\mathbb{X}_1, \mathbb{Y}_1), \cdots, (\mathbb{X}_N, \mathbb{Y}_N)\}$, are revealed. This data is used to check violation of Mermin's contextuality inequality given by (2).
7. The outcomes of other rounds are discarded.
8. If inequality (2) is violated, it implies the absence of eavesdropping and the sets of outcomes of $\mathbb{Z}_k$ work as a shared secure key.

Noise resilience of the protocol

- consider a channel between Bob_1 and Bob_2, in which noise is restricted to be some random unitary transformation $\mathbb{U}_1$. This noise only affects the statistics of observables of Bob_1 and leaves those of the subsequent Bobs, unchanged.
- The protocol starts with Bob_1 preparing a state $|\Psi'_M\rangle$. This is the state which is otherwise obtained after performing a random transformation $\mathbb{U}_1$ on the post-measurement state.
- Then he sends this state to Bob_2. Since the noise affects only the statistics of observables of Bob_1, which has been used for preparation of a state $|\Psi'_M\rangle$ only as a reference, there is no effect of noise on the protocol.
- Similarly, consider a noisy channel between Bob_k and Bob_{k+1} which can be represented by some random unitary transformation $\mathbb{U}_{1\cdots k}$.
- This noise only affects the statistics of the observables of the first k Bobs, which have already been measured, and, hence, the performance of the protocols is not affected.

In this way, contextuality-based QCPs are resilient to such noise. This unique feature is due to the commutativity of the observables of different Bobs.

References

[1] O Gühne, M Kleinmann, A Cabello, J Larsson, G Kirchmair, F Zähringer, R Gerritsma, and C.F. Roos. Phys. Rev. A, 81:022121, Feb 2010.
[2] N. David Mermin.Phys.Rev. Lett., 65:1838–1840, Oct 1990.
[3]MW Beijersbergen, RPC Coerwinkel, M Kristensen, and JP Woerdman.Optics communications, 112(5-6):321–327, 1994.
[4] Manuel Erhard, Robert Fickler, Mario Krenn, and Anton Zeilinger. 7(3):17146–17146, 2018.

Quantum Optics and Information Meeting: kobit $|5\rangle$