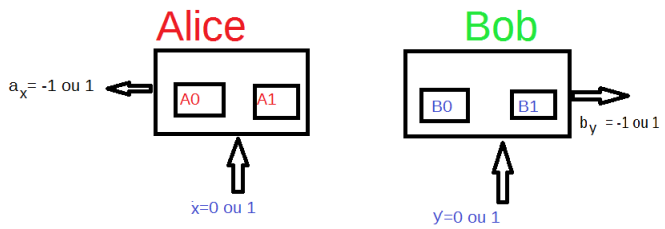
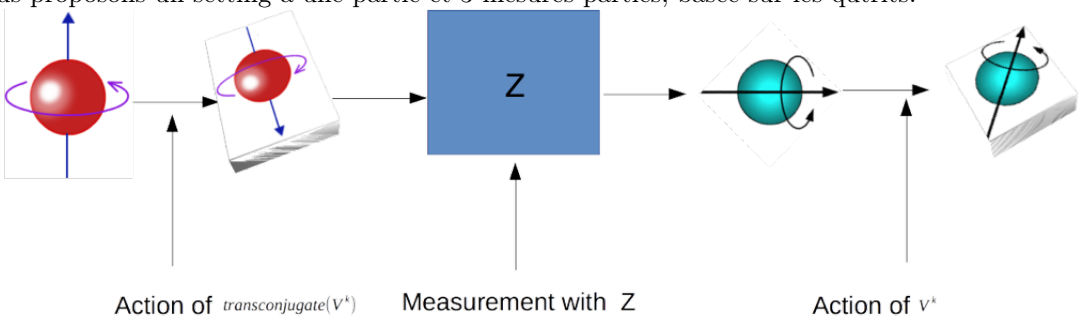
Génération quantique d'aléa et Intrication

Les nombres aléatoires sont une "denrée prisée" dans bien des domaines comme la simulation, les jeux de hasard, et en particulier en sécurité informatique. Pour ce faire, les séries de nombre produits ne doivent comporter aucun biais, être parfaitement aléatoires.
Mais, les procédés actuels de génération de nombre aléatoire sont basés sur des algorithmes pseudo aléatoires qui prennent en entrée des graines. Ces graines sont qualifiées de manière plus ou moins objectives "d'aléatoires". Dans le cadre de notre projet, nous proposons de baser le caractère aléatoire de nos expérience sur la base théorique solide qu'est la physique quantique. Ainsi, grâce aux caractères intrinsèques de la Physique quantique (les violations du réalisme local) nous donnons une borne sur la qualité des nombres produits au travers de l'outil qu'est l'entropie. Les résultats de base pour nos travaux sont ceux de S.Pironio et compagnie qui proposent un setting de 2 mesures par parties avec deux parties basé sur les qubits.



Nous proposons un setting à une partie et 3 mesures parties, basée sur les qutrits.



Ce setting offre une simplicité d'implémentation tout en restant dans le cadre du quantique, grâce à la violation des inégalités homogènes de Bell. Nous travaillons sur la quantification de l'aléa ainsi produit.

Bibliographie

[1] S. Pironio, A. Acín, S.Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe
" Random Numbers Certified by Bell's Theorem" *arXiv :0911.3427v3* 19 octobre 2010

[2] François Arnault "A complete set of multidimensional Bell inequalities", *J.PHYS. A : Math. Theor. 45 (2012) 255304 (18pp)*