FI264/F025 – Fundamentos da teoria quântica
Lista 9 – (02/2019)

1. Considere uma implementação de BB84 supostamente baseada em emaranhamento, em um cenário em que os dispositivos não são acessíveis. Supondo que Eva possa preparar os sistemas, proponha um estado ρ_{ABE}, compartilhado entre Alice, Bob e Eva, tal que as correlações

$$p\left(a=b|x=y\right)=1, \quad p\left(a=b|x\neq y\right)=1/2, \tag{1}$$

sejam observadas por Alice e Bob, e ao mesmo tempo, Eva tenha completo conhecimento da chave crua estabelecida.

2. Considere um protocolo de QKD implementado com um estado maximamente emaranhado $|\phi^+\rangle$ de dois qubits fotônicos. Alice e Bob extraem a chave medindo σ_z, e a segurança do protocolo é verificada em de forma independente de dispositivos através da violação de CHSH, com as medições ótimas para tal, assumindo-se ataques coletivos de uma Eva limitada pela teoria quântica. Assuma que os detectores das duas partes são ideais, e que a fonte fica no laboratório de Alice, de forma que todos os fótons endereçados a ela são detectados. Os fótons endereçados a Bob, no entanto, são detectados com probabilidade η; nas rodadas nas quais não há detecção, um resultado aleatório é escolhido.

   (a) Mostre que o valor previsto para a violação de CHSH é $S=\eta 2\sqrt{2}$.

   (b) Mostre que a fração de erros na chave crua é $\epsilon=p\left(a\neq b\right)=\left(1-\eta\right)/2$, e, portanto,

$$I\left(A:B\right)=1-h\left(\epsilon\right). \tag{2}$$

   (c) A fração secreta da chave é dada por

$$r=1-h\left(\epsilon\right)-h\left(\frac{1+\sqrt{\left(S/2\right)^2-1}}{2}\right). \tag{3}$$

   Calcule numericamente o valor crítico de η para que $r>0$.

   (d) Uma estimativa otimista para fibras óticas é $\eta=10^{-d/50}$, onde d é a distância, em kilômetros. Calcule a distância crítica para a implementação deste protocolo.

3. Considere um cenário de Bell $(2, 2, 2)$, no qual o detector de Bob não é ideal e um sistema local pode usufruir deste fato para emular comportamento não-local. Na tabela, estão listadas 8 estratégias locais que atingem o valor $S = 2$ para a desigualdade CHSH, onde a_x e b_y denotam os resultados das medições x e y, respectivamente, e $E(x, y)$ são os correlatores. O funcionamento dos detectores de Bob está correlacionado com o λ e com a medição escolhida: se algum dos valores entre parênteses é solicitado em alguma rodada do experimento, o detector funciona e retorna o resultado com probabilidade p, e não funciona com probabilidade $(1 - p)$. Suponha que em cada rodada valores de λ, x e y são sorteados uniformemente. Se apenas as rodadas nas quais o detector de Bob funciona são consideradas para estimar o comportamento das caixas, mostre que este comportamento leva a um valor de CHSH igual a $S = 4\frac{3-p}{3+p}$. Mostre também que há violação da desigualdade para todo $p > 0$.

	a_0	a_1	b_0	b_1	$E(0,0)$	$E(0,1)$	$E(1,0)$	$E(1,1)$
λ_1	0	0	0	(0)	1	(1)	1	(1)
λ_2	1	1	1	(1)	1	(1)	1	(1)
λ_3	0	0	0	(1)	1	(-1)	1	(-1)
λ_4	1	1	1	(0)	1	(-1)	1	(-1)
λ_5	0	1	(0)	0	(1)	1	(-1)	-1
λ_6	1	0	(1)	1	(1)	1	(-1)	-1
λ_7	0	1	(1)	0	(-1)	1	(1)	-1
λ_8	1	0	(0)	1	(-1)	1	(1)	-1