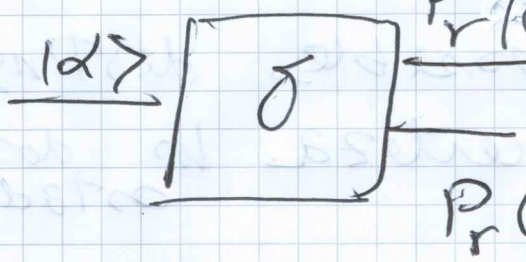
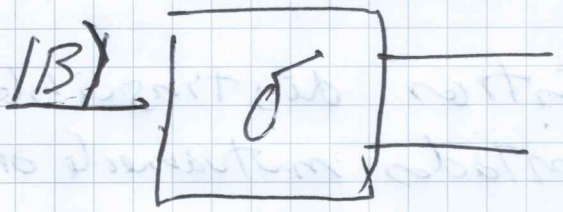
P4 Distinguibilidad de los estados $|\alpha\rangle$ y $|\beta\rangle$

(a) Si $\langle\alpha|\beta\rangle = 0$.



$= K|\langle\sigma_1|\alpha\rangle|^2 = 1$

$\Rightarrow |\sigma_1\rangle = |\alpha\rangle$



$= K|\langle\sigma_2|\beta\rangle|^2 = 1$

$\Rightarrow |\sigma_2\rangle = |\beta\rangle$

$$\sigma = \sigma_1 |\sigma_1\rangle\langle\sigma_1| + \sigma_2 |\sigma_2\rangle\langle\sigma_2|$$

$$\therefore \quad \sigma = \sigma_1 |\alpha\rangle\langle\alpha| + \sigma_2 |\beta\rangle\langle\beta|$$

A menos de un valor fijo y de una factor de escala: $\sigma_1 = -\sigma_2 = 1$

$$\boxed{\sigma = |\alpha\rangle\langle\alpha| - |\beta\rangle\langle\beta|}$$

(b) Si $\langle \alpha | \beta \rangle \neq 0$

Llegamos a lo mismo pero

$\langle \sigma_1 | \sigma_2 \rangle = 0$ por desc. espectral.

pero $|\sigma_1\rangle = |\alpha\rangle$, $|\sigma_2\rangle = |\beta\rangle$

$\Rightarrow \langle \alpha | \beta \rangle = 0$ Absurdo

$\therefore$ No es posible distinguir con certeza los dos estados.

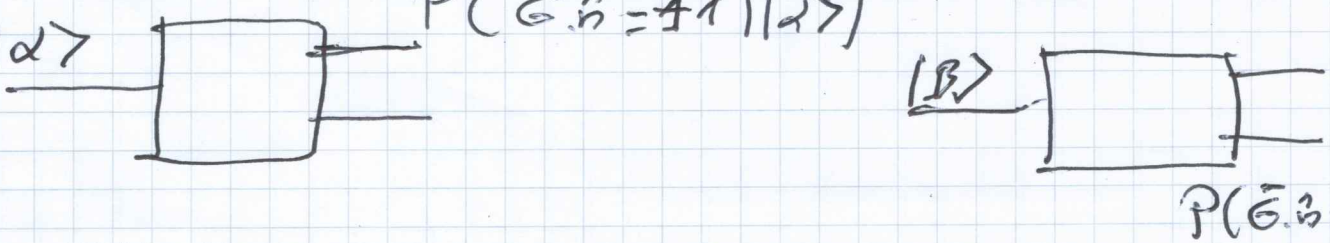
(c) "Los únicos estados cuánticos distinguibles con certeza son los estados mutuamente ortogonales"

(d) En $\mathbb{R}2$ cualquier estado está definido por una dirección $\hat{a}$ en la esfera de Bloch -

$$|\alpha\rangle = |+, \vec{\sigma}\cdot\hat{a}\rangle$$

$$|\beta\rangle = |+, \vec{\sigma}\cdot\hat{b}\rangle$$

Medimos: $\hat{\sigma}\cdot\hat{n}$ $\begin{cases} + \Rightarrow |\alpha\rangle \\ - \Rightarrow |\beta\rangle \end{cases}$



Cont. [P4] (d)

$$P_{rExito} = \underbrace{P_r(|\alpha\rangle)}_{P_r(|\alpha\rangle) \text{ y se mide } \vec{\sigma}\cdot\hat{n}=+1} P_r(\vec{\sigma}\cdot\hat{n}=+1 \,||\alpha\rangle) + \underbrace{P(|\beta\rangle)}_{P_r(|\beta\rangle \text{ y se mide } \vec{\sigma}\cdot\hat{b}=-1} \cdot P(\vec{\sigma}\cdot\hat{n}=-1 \,||\beta\rangle)$$

$$P_r(|\alpha\rangle) = \frac{1}{2} = P_r(|\beta\rangle)$$

Usaremos:

$$P_r(\vec{\sigma}\cdot\hat{n}=+1 \mid \vec{\sigma}\cdot\hat{a}=+1) = \langle +,\vec{\sigma}\cdot\hat{a}| \underbrace{|+\vec{\sigma}\cdot\hat{n}\rangle\langle+\vec{\sigma}\cdot\hat{n}|}_{\Pi_{+\hat{n}}} |+\vec{\sigma}\cdot\hat{a}\rangle$$

$$= Tr\left(\Pi_{+\hat{n}} \cdot \Pi_{+\hat{a}}\right)$$

$$= Tr\left[\frac{(1+\vec{\sigma}\cdot\hat{n})}{2}\cdot\frac{(1+\vec{\sigma}\cdot\hat{a})}{2}\right]$$

$$= \frac{1}{4} Tr\left[\mathbb{1} + \underbrace{\vec{\sigma}\cdot\hat{n}\,\vec{\sigma}\cdot\hat{a}}_{\hat{n}\cdot\hat{a}\,\mathbb{1} + (\hat{n}\times\hat{a})\cdot\vec{\sigma}} + \underbrace{\vec{\sigma}\cdot\hat{n} + \vec{\sigma}\cdot\hat{a}}_{tr=0}\right]$$

6. $P_r(\vec{\sigma}\cdot\hat{n}=+a \mid \vec{\sigma}\cdot\hat{a}=+1) = \frac{1}{2}(1+\hat{n}\cdot\hat{a})$!

Del mismo modo:

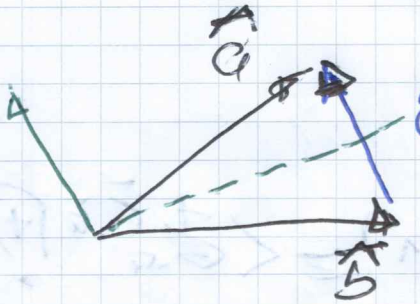
$$Pr(\vec{G}\cdot\hat{a} = -1 \,|\, \vec{G}\cdot\hat{b} = +1) = Tr(\Pi_{-\hat{a}}\,\Pi_{+\hat{b}})$$

$$= Tr\left[\frac{1}{2}(1-\vec{G}\cdot\hat{a})\frac{1}{2}(1+\vec{G}\cdot\hat{b})\right]$$

$$= \frac{1}{2}(1-\hat{a}\cdot\hat{b})$$

$$\therefore P_{exito} = \frac{1}{2} + \frac{1}{4}\hat{n}\cdot(\hat{a}-\hat{b})$$

Es máxima si $\hat{n} \parallel \hat{a}-\hat{b}$



Máxima $\hat{n}\cdot(\hat{a}-\hat{b}) = |\hat{n}|\,|\hat{a}-\hat{b}|\underbrace{\cos 0}_{1} = \sqrt{(\hat{a}-\hat{b})^2}$

$$\therefore \hat{n}\cdot(\hat{a}-\hat{b}) = \sqrt{|\hat{a}|^2+|\hat{b}|^2-2\hat{a}\cdot\hat{b}}$$

$$= \sqrt{2(1-\hat{a}\cdot\hat{b})}$$

$$P_{Máxima} = \frac{1}{2} + \frac{1}{2\sqrt{2}}\sqrt{1-\hat{a}\cdot\hat{b}}$$

i) Si $\hat{b} = -\hat{a}$ (ortogonales $\langle a|b\rangle = 0$) $P_{máxima} = 1$

ii) Si $\hat{b} \perp \hat{a}$ $P_{máxima} = \frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right) \simeq 0.85$.

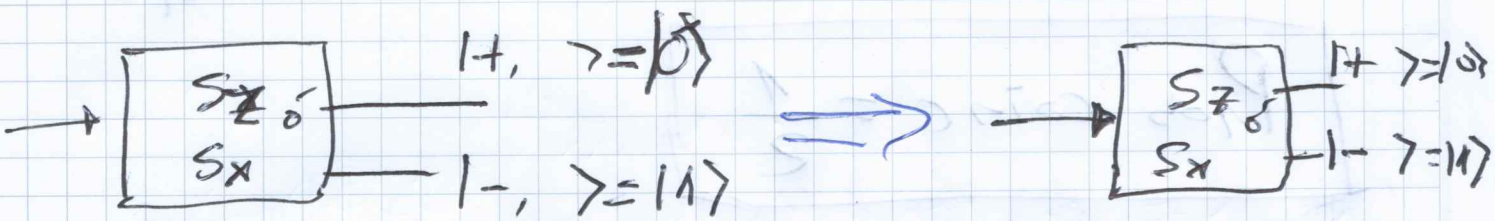
iii) Si $\hat{b} \simeq -\hat{a}$ $P \simeq 1$

P5 Criptografía Cuántica

Distribución Cuántica de Claves

Protocolo BB84

(Bennet-Brassard 1984)



Alice

Base Estado

Bob

Base Estado

Para obtener el mismo estado (auto estado del mismo operador)

Deben coincidir en el operador:

Alice	Bob	
S_z	S_z	
S_z	S_x	$\frac{1}{2}$ de los veces coinciden en la base (operador)
S_x	S_z	
S_z	S_z	

(b) • Si miden en la misma base (el mismo observable)

$$P(\text{medir lo mismo} \mid \text{mismo } \vec{S}\cdot\hat{n}) = 1$$

$$P_{\text{prob. coinc.}} = \underbrace{P(\text{mismo } \vec{S}\cdot\hat{n})}_{1/2} \cdot \underbrace{P(\text{medir lo mismo} \mid \text{mismo } \vec{S}\cdot\hat{n})}_{1}$$

$$\boxed{P_{\text{prob coinc}} = \frac{1}{2}}$$

• Si miden distinto observable.

$$P(\text{medir distinto } \vec{S}\cdot\hat{n}) = 1/2$$

$$P(\text{medir lo mismo} \mid \text{distinto } \vec{S}\cdot\hat{n}) = \frac{1}{2}$$

$$\boxed{P_{\text{prob coinc}} = \frac{1}{4}}$$

$$P_{\text{prob coinc total}} = \frac{3}{4}$$

Para asegurar la misma correlación se toman sólo los pares medidos con el mismo operador (publicados por Alice)

$$0 \to |+, \vec{S}\cdot\hat{n}\rangle \quad 1 \to |-, \vec{S}\cdot\hat{n}\rangle \quad \vec{S}\cdot\hat{n} \langle S_x \; S_z$$

(c) Aparece Eve (Eavesdropper)
"Espía"

Prob Eve mide en la misma base que Alice $= \frac{1}{2}$

Si recuerda el estado como midió. entonces en cada evento la Prob. $= \frac{1}{2}$ de acertar el correcto estado.

Pero Eve necesita que la secuencia sea correcta:

$$P_{\text{éxito }1} \cdot P_{\text{éxito }2} \cdot P_{\text{éxito }3} \cdots$$

$$\simeq \left(\frac{1}{2}\right)^{N \text{ clave}}.$$

$\Rightarrow$ La probabilidad de al menos un error es grande $(1 - P_{\text{éxito}})$

Bob y Alice pueden detectar la diferencia y descartan toda la secuencia.