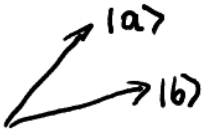
Lecture 3 — Quantum Crypto

3.1 Information encoded in quantum states is different



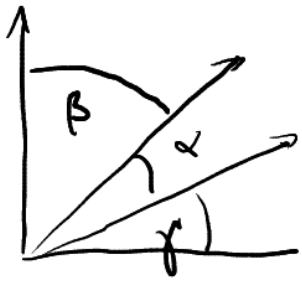
$\langle a|b\rangle = r$ — the two states cannot be reliably distinguished

NO CLONING → non-orthogonal states cannot be cloned

$|a\rangle|0\rangle|e\rangle \rightarrow |a\rangle|a\rangle|e_a\rangle$
$|b\rangle|0\rangle|e\rangle \rightarrow |b\rangle|b\rangle|e_b\rangle$

inner prod. $\langle a|b\rangle = r \qquad r = 1^2\langle e_a|e_b\rangle = r=0,\ r=1,\ \langle e_a|e_b\rangle = 1$

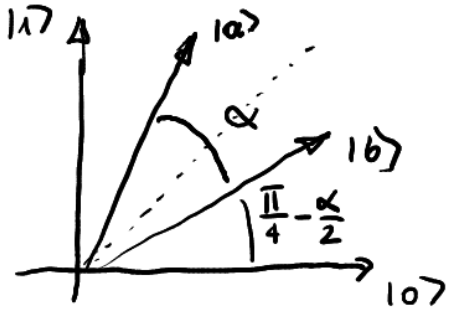
3.2 OPTIMAL STATE DETECTION



$|0\rangle, |b\rangle$ prepared with a priori prob $\frac{1}{2}$

minimise $\sin^2\beta + \sin^2\gamma$ α fixed

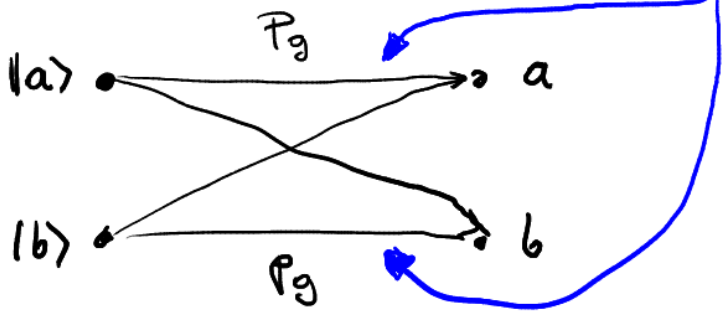
symmetry arguments



Probability of correct guess

$$= \cos^2\left(\frac{\pi}{4} - \frac{\alpha}{2}\right)$$
$$= \left[\cos\frac{\pi}{4}\cos\frac{\alpha}{2} + \sin\frac{\pi}{4}\sin\frac{\alpha}{2}\right]^2$$
$$= \left[\frac{1}{\sqrt{2}}\left(\cos\frac{\alpha}{2} + \sin\frac{\alpha}{2}\right)\right]^2$$
$$= \frac{1}{2}(1+\sin\alpha)$$
$$= \frac{1}{\sqrt{2}}\left(1 + \sqrt{1-|\langle a|b\rangle|^2}\right)$$

$$P_{correct} = \frac{1}{2}(1+\sin\alpha) = \frac{1}{2}\left(1+\sqrt{1-|\langle a|b\rangle|^2}\right)$$



3.3 ENTANGLED STATES

$$\Phi^{\pm} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \quad \Psi^{\pm} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$$

SWITCHING BETWEEN BASES

$$|0\rangle = \frac{1}{\sqrt{2}}(|\bar{0}\rangle + |\bar{1}\rangle), \quad |1\rangle = \frac{1}{\sqrt{2}}(|\bar{0}\rangle - |\bar{1}\rangle)$$

$$\Phi^{+} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}\left(\begin{matrix} |\bar{0}\bar{0}\rangle + |\bar{0}\bar{1}\rangle + |\bar{1}\bar{0}\rangle + |\bar{1}\bar{1}\rangle \\ |\bar{0}\bar{0}\rangle - |\bar{0}\bar{1}\rangle - |\bar{1}\bar{0}\rangle + |\bar{1}\bar{1}\rangle \end{matrix}\right)$$

$$= \frac{1}{\sqrt{2}}(|\bar{0}\bar{0}\rangle + |\bar{1}\bar{1}\rangle) \leftarrow \text{INVARIANT}$$

THE ONLY SUCH STATE

$$\Phi^{+} \longleftrightarrow \Phi^{+}, \quad \Phi^{-} \longleftrightarrow \Psi^{+}, \quad \Psi^{-} \longleftrightarrow -\Psi^{-}$$

3.4

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)|e\rangle \longrightarrow \frac{1}{\sqrt{2}}(|00\rangle|e_0\rangle + |11\rangle|e_1\rangle)$$

$$= \Phi^{+}\frac{|e_0\rangle + |e_1\rangle}{2} + \Phi^{-}\frac{|e_0\rangle - |e_1\rangle}{2}$$

$$\Phi^{+}\frac{|e_0\rangle + |e_1\rangle}{2} + \Psi^{+}\frac{|e_0\rangle - |e_1\rangle}{2}$$

Eavesdropping

$\longrightarrow$ DIAGONAL BASIS

$$Q = \frac{1}{2}(1 - r)$$

$$P_g = \frac{1}{2}\left(1 + \sqrt{1 - r^2}\right)$$

$$= \frac{1}{2} + \sqrt{\left(\frac{1-r}{2}\right)\left(\frac{1+r}{2}\right)} = \frac{1}{2} + \sqrt{Q(1-Q)}$$

PROB OF GUESSING CORRECTLY VS DISTURBANCE

3.4 MORE GENERAL CASE

$1/\sqrt{2}$ $1/\sqrt{2}$

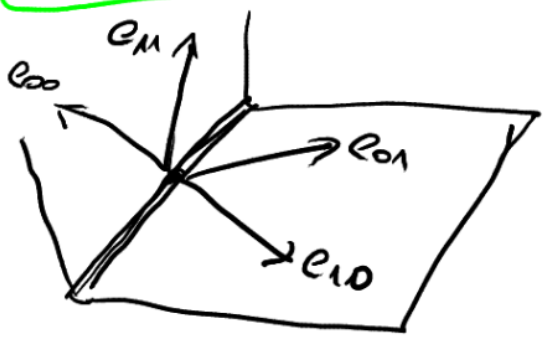
$$\sqrt{A}\left(|00\rangle|e_{00}\rangle + |11\rangle|e_{11}\rangle\right) + \sqrt{B}\left(|01\rangle|e_{01}\rangle + |10\rangle|e_{10}\rangle\right)$$

$$\sqrt{A}\left(\Phi^{+}\frac{|e_{00}\rangle + |e_{11}\rangle}{2} + \Phi^{-}\frac{|e_{00}\rangle - |e_{11}\rangle}{2}\right) + \sqrt{B}\left(\Psi^{+}\frac{|e_{01}\rangle + |e_{10}\rangle}{2} + \Psi^{-}\frac{|e_{01}\rangle - |e_{10}\rangle}{2}\right)$$

$$\sqrt{A}\left(\Phi^{+}\left(\frac{|e_{00}\rangle + |e_{11}\rangle}{2}\right) + \Psi^{+}\left(\frac{|e_{00}\rangle - |e_{11}\rangle}{2}\right)\right) + \sqrt{B}\left(\Phi^{-}\left(\frac{|e_{01}\rangle + |e_{10}\rangle}{2}\right) - \Psi^{-}\left(\frac{|e_{01}\rangle - |e_{10}\rangle}{2}\right)\right)$$

$$A+B=1$$
$$A-B = Aa+Bb$$

$$A\tfrac{1}{2}(1-a)+B\tfrac{1}{2}(1-b) = B$$



The same disturbance in the new basis

$$P_g = A\left(\tfrac{1}{2}+\tfrac{1}{2}\sqrt{1-a^2}\right)+B\left(\tfrac{1}{2}+\tfrac{1}{2}\sqrt{1-b^2}\right)$$
$$= \tfrac{1}{2}\left(1+A\sqrt{1-a^2}+B\sqrt{1-b^2}\right)$$

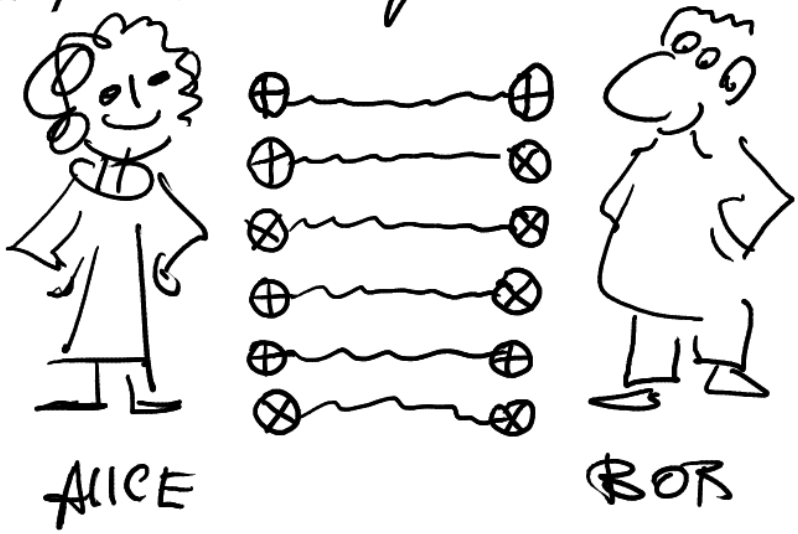
Maximize P_g given $A+B=1$ and $A(1-a) = B(1+b)$

max for
$a=b$
$A+B=1$
$A-B=a$
$\frac{1-a}{2}=B$

$$P_g = \tfrac{1}{2}\left(1+\sqrt{1-a^2}+B\left(\sqrt{1-b^2}-\sqrt{1-a^2}\right)\right)$$
$$P_g = \tfrac{1}{2}+\sqrt{B(1-B)}$$

$$P_g = \tfrac{1}{2}+\sqrt{Q(1-Q)}$$ ✓

3.5 Key distribution protocol



DISTRIBUTE Φ^+
MEASURE $\oplus, \otimes$
ESTIMATE Q, P_g
DISTILL KEY