10- Individual attack

26 października 2010
12:05

Optimal individual attack on BB84

$$|\psi\rangle = \begin{cases} |0\rangle \\ |1\rangle \\ |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$$

$|\psi\rangle_A$, $|0\rangle_E$ → U → $|\Psi\rangle_{BE}$ — B; Π_i — E

↑ ent state between A & E

$$U: \mathcal{H}_A \otimes \mathcal{H}_E \to \mathcal{H}_B \otimes \mathcal{H}_E$$

$\dim \mathcal{H}_A = 2$ ↑ $\dim \mathcal{H}_E$ a priori can be arbitrary $\dim \mathcal{H}_B = 2$

10.1 Intuition

To get some intuition consider the following attack

$$\begin{cases} |0\rangle_A \otimes |a\rangle_E \to |0\rangle_B \otimes |a\rangle_E \\ |1\rangle_A \otimes |a\rangle_E \to |1\rangle_B \otimes |\Theta\rangle_E \end{cases} \qquad |\Theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$$

If $\theta = 0$, E gains no information, if $\theta = \frac{\pi}{2}$ E gains full information on $|a\rangle_E|\psi\rangle_A$. In either case B state are undisturbed

How this operation acts on $|+\rangle, |-\rangle$

$$|+\rangle_A \otimes |a\rangle_E \to \frac{1}{\sqrt{2}}\left(|0\rangle_B \otimes |a\rangle_E + |1\rangle_B \otimes |\Theta\rangle_E\right) = |\Psi^+\rangle_{BE}$$

$$|-\rangle_A \otimes |a\rangle_E \to \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |a\rangle - |1\rangle \otimes |\Theta\rangle\right) = |\Psi^-\rangle_{BE}$$

Let us look at reduced density matrices of B and E

$$|+\rangle_A\langle+| = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

$$\rho_B^+ = Tr_E\left(|\psi^+\rangle_{BE}\langle\psi^+|\right) = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|0\rangle\langle 1| \cdot \underbrace{\langle\Theta|0\rangle}_{\cos\theta} + \frac{1}{2}|1\rangle\langle 0| \underbrace{\langle 0|\Theta\rangle}_{\cos\theta} + \frac{1}{2}|1\rangle\langle 1| =$$

$$= \frac{1}{2}\begin{bmatrix} 1 & \cos\theta \\ \cos\theta & 1 \end{bmatrix}$$ — we are loosing coherence in particular for $\theta = \frac{\pi}{2}$ $\rho_B^+ = \frac{1}{2}\mathbb{1}$

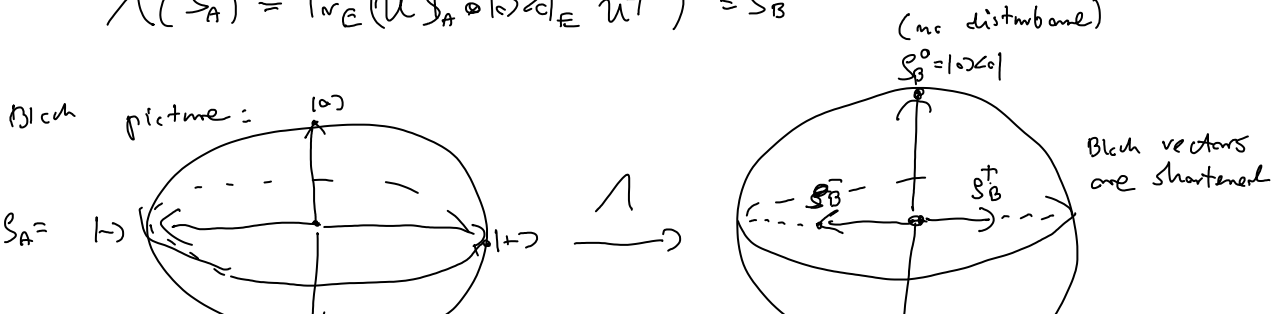
$$\rho_B^- = \frac{1}{2}\begin{bmatrix} 1 & -\cos\theta \\ -\cos\theta & 1 \end{bmatrix} \qquad \rho_B^+ = \cos^2\frac{\theta}{2}|+\rangle\langle+| + \sin^2\frac{\theta}{2}|-\rangle\langle-|$$

$$\begin{bmatrix} 1 & \pm\cos\theta \\ \pm\cos\theta & 1 \end{bmatrix} \qquad \rho_B^- = \cos^2\frac{\theta}{2}|-\rangle\langle-| + \sin^2\frac{\theta}{2}|+\rangle\langle+|$$

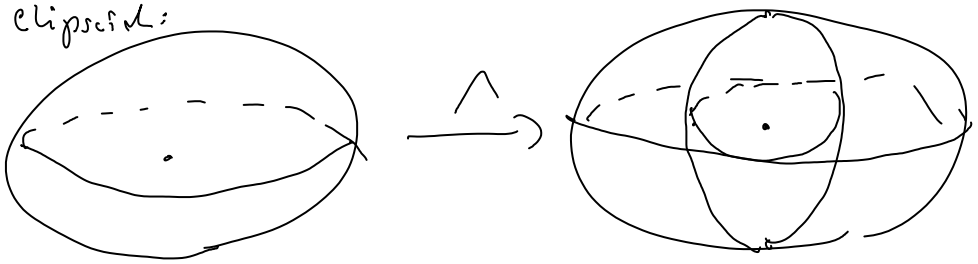
The more E learns about B in $|a\rangle, |\bar{a}\rangle$ basis the bigger disturbance it causes in $|+\rangle, |-\rangle$ basis.

Let us look at the transformation restricted to B(A) subsystem

$$\Lambda(\rho_A) = Tr_E\left(U \rho_A \otimes |a\rangle\langle a|_E U^\dagger\right) = \rho_B$$



If you looked at all states the CP map would transform Bloch ball into ellipsoid:

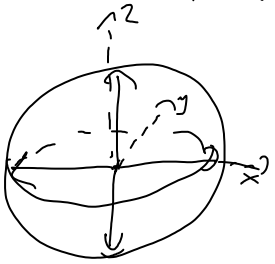


(Notice also that $\rho_E^+ = \rho_E^- = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ - E cares nothing in $|+\rangle, |-\rangle$ basis)

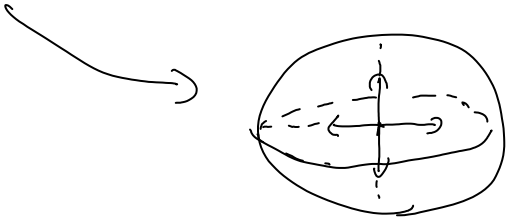
10.2 Symmetry

The above attack breaks the symetry of the protocol. It is natural to assume that the optimal attack should be "symmetric" - do not distinguish any of the states.

How we can transform 4 Bloch vectors in symmetric way

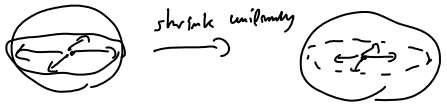


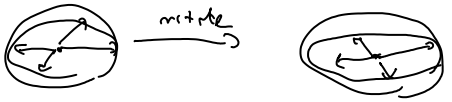
- if a rotation then only rotation around y-axis Unitary rotation would increase QBER, and since it is invertible E would always invert it.
- shrinking of Bloch vectors



More formally: (From a nonsymmetric attack we can make a symmetric without losing information nor increasing QBER)

What kind of operation are D_2 covariant. Let four states be on the equator for clearer picture





- can be reversed, decreasing QBER

- can be mixed with

so effectively we go back to equatorial plane without changing QBER

So only symmetric shrinking !

In summary:

- E rotates randomly the state from A by $0, \pm 90, 180, 270°$ (on Bloch sphere)
- After the interaction and labeling her probe she rotates back the state sent to B

This means that four states received by B must by symmetric with respect to such rotations: If they are not in big circle plane E could generalize her attack, and randomly choose an attack that produce states in the upper or lower hemisphere (this does not change QBER, nor her info)

Symetry:

$$|\psi\rangle_A\langle\psi| \xrightarrow{\Lambda} \eta\,|\psi\rangle_B\langle\psi| + (1-\eta)\,|\psi^\perp\rangle_B\langle\psi^\perp|$$

10.3 optimal symmetric attack

$$|0\rangle_A \otimes |0\rangle_E \xrightarrow{U} \alpha_{00}|0\rangle_B \otimes |e_{00}\rangle_E + \alpha_{01}|1\rangle_B \otimes |e_{01}\rangle_E$$

$$|1\rangle_B \otimes |0\rangle_E \xrightarrow{U} \alpha_{11}|1\rangle_B \otimes |e_{11}\rangle_E + \alpha_{10}|0\rangle_B \otimes |e_{10}\rangle_E$$

We assume $\alpha_{ij} \in \mathbb{R}$, all scalar products $\langle e_{ij}|e_{i'j'}\rangle \in \mathbb{R}$
(can be justified, reason is that all states in BB84 use real coef)

$$\rho_B^0 = \alpha_{00}^2 |0\rangle\langle 0| + \alpha_{01}^2 |1\rangle\langle 1| + \alpha_{00}\alpha_{01}\langle e_{01}|e_{00}\rangle\left(|0\rangle\langle 1| + |1\rangle\langle 0|\right)$$

by symetry assumption (shrinking of Bloch vector):

i) $\langle e_{00}|e_{01}\rangle = 0$, $\langle e_{11}|e_{10}\rangle = 0$

$\alpha_{00} = \alpha_{11} = \sqrt{F}$ ← fidelity

$\alpha_{01} = \alpha_{10} = \sqrt{E}$ ← prob of error

by normalization $F + E = 1$

ii) by unitarity

$$\sqrt{FE}\cdot\left(\langle e_{00}|e_{10}\rangle + \langle e_{01}|e_{11}\rangle\right) = 0$$

	e_{00}	e_{01}	e_{10}	e_{11}
e_{00}	1	0	x	y
e_{01}	0	1	z	v
e_{10}	x	z	1	0
e_{11}	y	v	0	1

iii) by symetry we know that the transformation

should look the same in $|+\rangle, |-\rangle$ basis i.e

$$|+\rangle \otimes |0\rangle_E \xrightarrow{U} \sqrt{F}\,|+\rangle|e_{++}\rangle + \sqrt{E}\,|-\rangle|e_{+-}\rangle$$

$$|-\rangle \otimes |0\rangle \longrightarrow \sqrt{F}\,|-\rangle|e_{--}\rangle + \sqrt{F}\,|+\rangle|e_{-+}\rangle$$

But the action on $|+\rangle|0\rangle, |-\rangle|0\rangle$ is determined by action on $|0\rangle|0\rangle, |1\rangle|0\rangle$ since by linearity

$$|+\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|0\rangle\right) \xrightarrow{U}$$

$$\longrightarrow \frac{1}{\sqrt{2}}\left(\sqrt{F}\,|0\rangle|e_{00}\rangle + \sqrt{E}\,|1\rangle|e_{01}\rangle + \sqrt{F}\,|1\rangle|e_{11}\rangle + \sqrt{E}\,|0\rangle|e_{10}\rangle\right)$$

$$\begin{cases} |0\rangle = \dfrac{|+\rangle + |-\rangle}{\sqrt{2}} \\ |1\rangle = \dfrac{|+\rangle - |-\rangle}{\sqrt{2}} \end{cases}$$

$$= \underbrace{|+\rangle \otimes \frac{1}{2}\left(\sqrt{F}\,|e_{00}\rangle + \sqrt{E}\,|e_{01}\rangle + \sqrt{F}\,|e_{11}\rangle + \sqrt{E}\,|e_{10}\rangle\right)}_{\sqrt{F}\,|e_{++}\rangle} +$$

$$+ \underbrace{|-\rangle \otimes \frac{1}{2}\left(\sqrt{F}\,|e_{00}\rangle - \sqrt{E}\,|e_{01}\rangle - \sqrt{F}\,|e_{11}\rangle + \sqrt{E}\,|e_{10}\rangle\right)}_{\sqrt{E}\,|e_{+-}\rangle}$$

$$\langle e_{++}|e_{+-}\rangle = 0$$

$$\Downarrow$$

$$F\left(\underbrace{\langle e_{11}|e_{00}\rangle}_{0} - \langle e_{01}|e_{11}\rangle\right) + E\left(\langle e_{01}|e_{10}\rangle - \underbrace{\langle e_{10}|e_{01}\rangle}_{0}\right)$$

$$+ \sqrt{EF}\cdot\left(\langle e_{00}|e_{10}\rangle - \langle e_{11}|e_{01}\rangle + \langle e_{10}|e_{00}\rangle - \langle e_{01}|e_{11}\rangle\right) = 0$$

$$\Downarrow$$

v) $\sqrt{EF}\left(\langle e_{00}|e_{10}\rangle - \langle e_{11}|e_{01}\rangle\right) = 0$

together with (ii) this gives $\langle e_{00}|e_{10}\rangle = \langle e_{11}|e_{01}\rangle = 0$

additionally

vi) $\langle e_{++}|e_{++}\rangle = 1$

$$(1-E)\langle e_{11}|e_{00}\rangle + E\langle e_{01}|e_{10}\rangle + \sqrt{EF}\underbrace{\left(\langle e_{00}|e_{10}\rangle + \langle e_{11}|e_{01}\rangle\right)}_{0 \text{ by (ii)}} = 1 - 2E$$

	e_{00}	e_{01}	e_{10}	e_{11}
e_{00}	1	0	0	y
e_{01}	0	1	z	0
e_{10}	0	z	1	0
e_{11}	y	0	0	1

$$(1-E)\cdot y + E\cdot z = 1-2E$$

$$z = \frac{1}{E} - \frac{y(1-E)}{E} - 2$$

- Let us maximize $I(A:E)$

Notice that $\mathrm{span}(|e_{00}\rangle, |e_{11}\rangle) \perp \mathrm{span}(|e_{01}\rangle, |e_{10}\rangle)$

So E can make first a measurement projecting on this two subspaces – She learns whether B received an error or not.

Now in order to learn bit of A she need to distinguish between two nonorthogonal states:

Prob of error: $\langle \psi_1 | \psi_2 \rangle = x$ $\quad p(x) = \frac{1}{2}\left(1 - \sqrt{1 - x^2}\right)$

$$I(A:E) = (1-E)\cdot\left[1 - h(p(y))\right] + E\left[1 - h(p(z))\right]$$

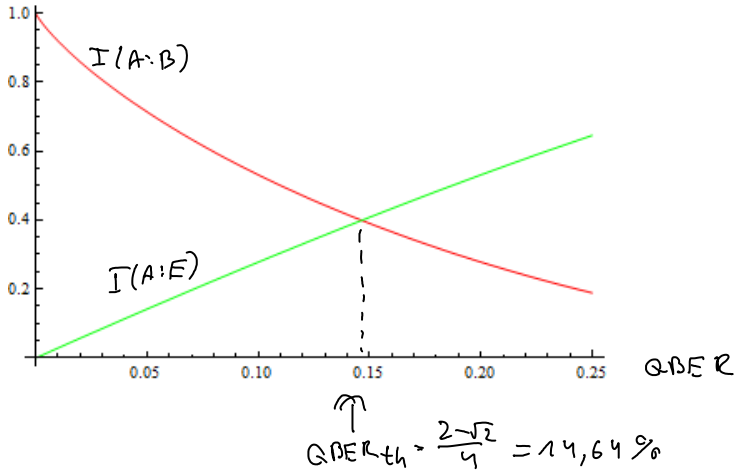
$$= (1-E)\left[1 - h(p(y))\right] + E\left[1 - h\left(p\left(\frac{1}{E} - \frac{y(1-E)}{E} - 2\right)\right)\right]$$

$$\frac{d\,I(A:E)}{dy} = -(1-E)\,h'(p(y))\,p'(y) + E\,h'(p(z))\,p'(z)\,\frac{1-E}{E} = 0$$

maximum is achieved for $z = y = 1 - 2E$

$$I(A:E) = 1 - h\left(\frac{1}{2}\left(1 - 2\sqrt{E(1-E)}\right)\right)$$

$$I(A:B) = 1 - h(E)$$



$QBER_{th} = \frac{2-\sqrt{2}}{4} = 14{,}64\,\%$