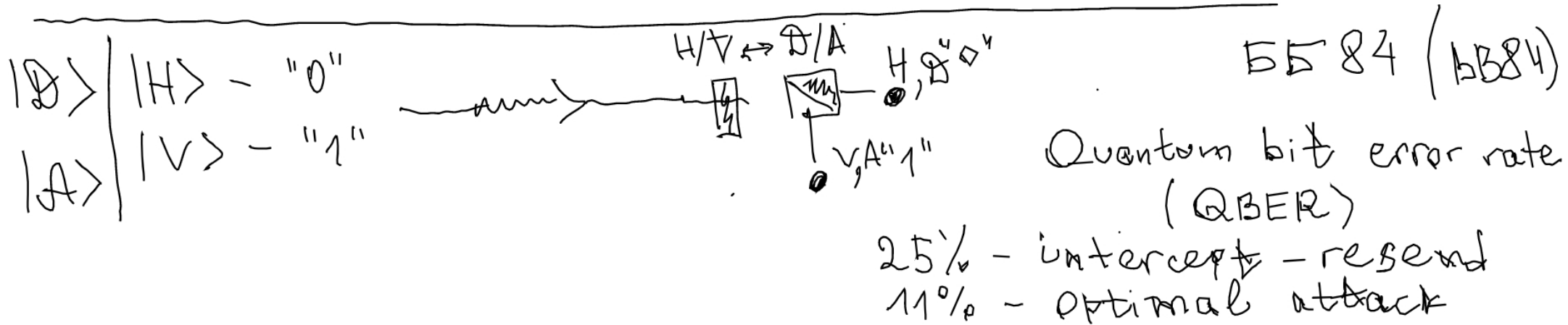
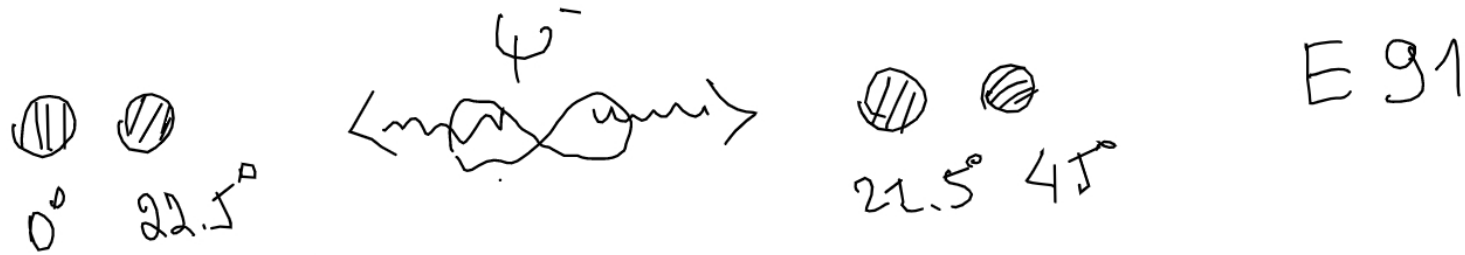


Кл. распр. ключа (КРК) QKD



- 1 сыфр. код (raw)
- 2 corr. базисов (reconciliation) → просеянный код
- 3 пер. фидбек (err. cor)
- 4 усиление секр. (privacy ampl)

$$|\psi\rangle \rightarrow |\psi\rangle_B |\psi\rangle_E$$

$$|\psi\rangle \rightarrow |\psi\rangle |\psi\rangle$$

$$\langle \psi | \psi \rangle = \langle \psi | \psi \rangle^2$$

$$\langle \psi | \psi \rangle = 0$$

$$\langle \psi | \psi \rangle = 1$$

"no-cloning"

$$\{ |H\rangle, |V\rangle, |D\rangle, |A\rangle \}$$

$$|\psi\rangle \rightarrow |\tilde{\psi}_1\rangle |\tilde{\psi}_2\rangle$$

$$|H\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

1 $\rightarrow H, V$

2 $\rightarrow D, A$

$$\frac{1}{\sqrt{2}} (|H\rangle + |V\rangle)$$

$$\frac{1}{2} |H\rangle \langle H| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\frac{1}{2} |V\rangle \langle V| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\left\{ \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix} \right\}$$

$$|D\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} |H\rangle + |V\rangle \\ H - V \end{pmatrix}$$

$$|D\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$|A\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$\langle D| = \frac{1}{\sqrt{2}} (1 \ 1)$$

$$\langle A| = \frac{1}{\sqrt{2}} (1 \ -1)$$

$$|D\rangle \langle D| = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

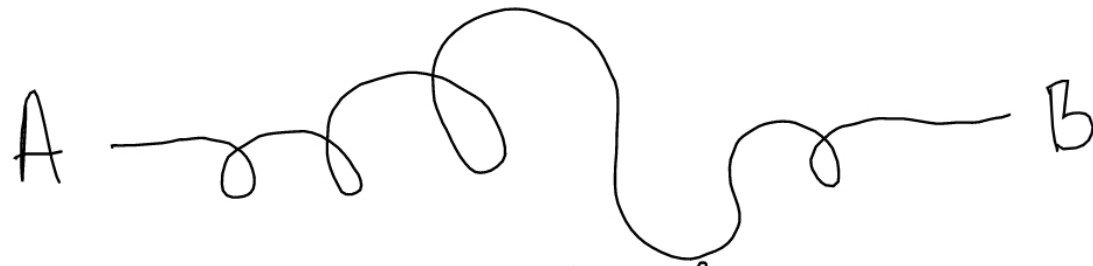
$$|A\rangle \langle A| = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

$$\frac{1}{2} |D\rangle \langle D| + \frac{1}{2} |A\rangle \langle A| = \frac{1}{4} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\{H, V\}$$

$$\{D, A\}$$

NOTE:



0.2 dB/km

потери в волокно: 100 pаз / 100 km

{H, V}

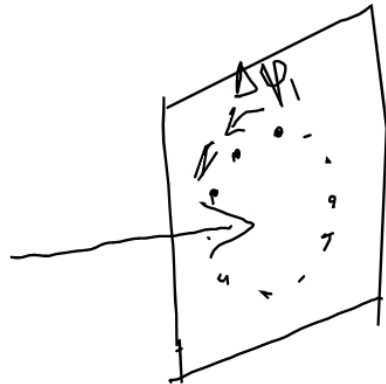
{D, A}

{R, L}

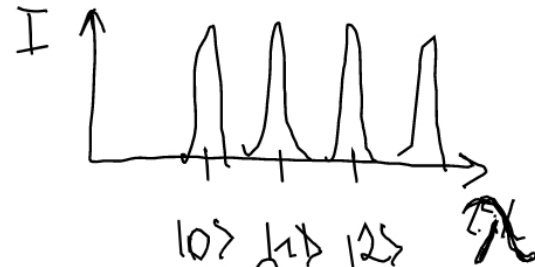
$$\frac{1}{3} \cdot 0 + \frac{2}{3} \cdot \frac{1}{2} = \frac{1}{3} = 33\%$$

$$\frac{1}{2} \cdot 0 + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} = 25\%$$

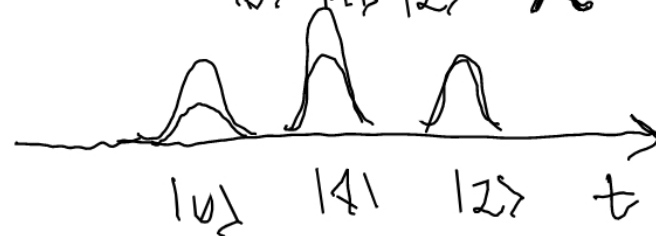
q-dit



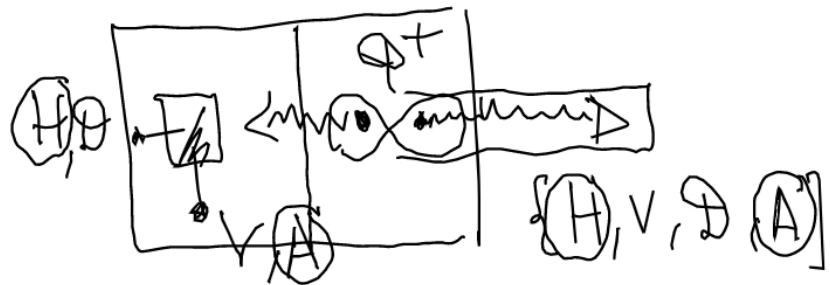
$$\sum \Delta \psi_i = 2\pi \cdot N$$



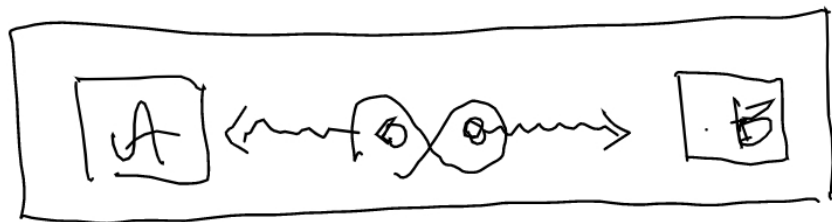
frequency bin



time bin



ent-based



q. repeater

