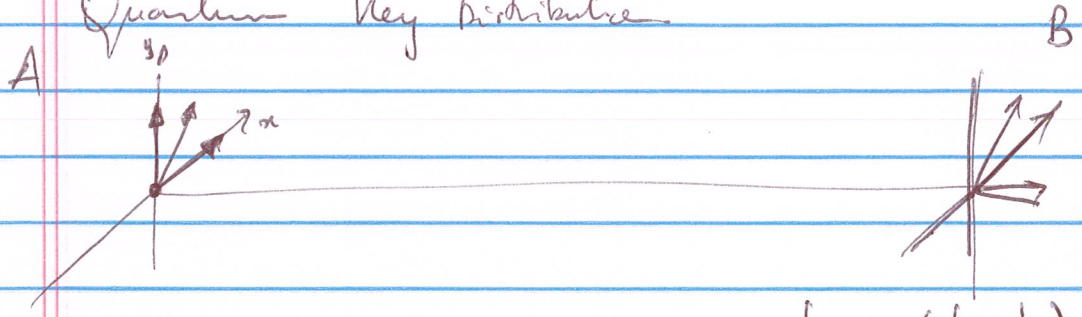
Quantum Key distribution



$a_1 = (0, 1)$

$a_2 = (1/\sqrt{2}, 1/\sqrt{2})$

$a_3 = (1, 0)$

$b_1 = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$

$b_2 = (1, 0)$

$b_3 = (1/\sqrt{2}, -1/\sqrt{2})$

(a_2, b_1)

(a_3, b_2)

$$P_{++}(a_i, b_j) = \frac{1}{4} - \frac{1}{4} a_i \cdot b_j$$

$$P_{--}(a_i, b_j) = \frac{1}{4} - \frac{1}{4} a_i \cdot b_j$$

$$P_{+-}(a_i, b_j) = \frac{1}{4} + \frac{1}{4} a_i \cdot b_j$$

$$P_{-+}(a_i, b_j) = \frac{1}{4} + \frac{1}{4} a_i \cdot b_j$$

$a_3 \to a_1$, $b \to -b$

$$P_{++} + P_{--} + P_{+-} + P_{-+} = 1 \quad \checkmark$$

correlation coeff.

$$E(a_i, b_j) = P_{++} + P_{--} - P_{+-} - P_{-+} = -a_i \cdot b_j$$

$$E(a_2, b_1) = -1 = E(a_3, b_2)$$

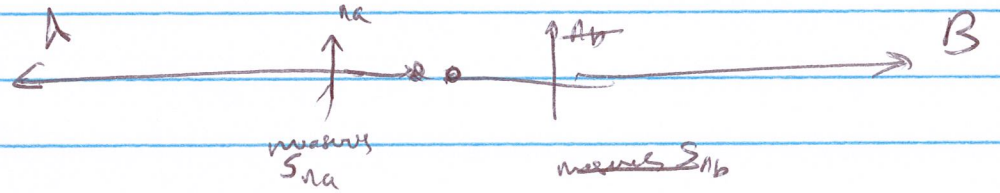
$$S = E(a_1, b_1) - E(a_1, b_3) + E(a_3, b_1) + E(a_3, b_3)$$

$$= -1/\sqrt{2} - 1/\sqrt{2} - 1/\sqrt{2} - 1/\sqrt{2} = \boxed{-2\sqrt{2}}$$

Pairs (a_2, b_1) (a_3, b_2) are used to have a common key for encoding

Pairs (a_1, b_1) (a_1, b_3) (a_3, b_1) (a_3, b_3) are used to check S.

Ecnes, dropping



§ $|\psi\rangle$ = not pure anymore

$1/2 \rightarrow |\uparrow_{n_a} \downarrow_{n_a}\rangle$

$1/2 \rightarrow |\downarrow_{n_a} \uparrow_{n_a}\rangle$

$$P_{+-}(a_i, b_j) = \frac{1}{2} |\langle \uparrow_{a_i} | \uparrow_{n_a} \rangle|^2 |\langle \uparrow_{b_j} | \downarrow_{n_a} \rangle|^2 +$$

$$+ \frac{1}{2} |\langle \uparrow_{a_i} | \downarrow_{n_a} \rangle|^2 |\langle \uparrow_{b_j} | \uparrow_{n_a} \rangle|^2$$

$$= \frac{1}{8}(1 - a_i n_a)(1 + b_j n_a) + \frac{1}{8}(1 + a_i n_a)(1 - b_j n_a)$$

$$= \frac{1}{4} - \frac{1}{4}(a_i n_a)(b_j n_a)$$

$$P_{++} = \frac{1}{4} - \frac{1}{4}(a_i \cdot n_a)(b_j \cdot n_a)$$

$$P_{--} = \frac{1}{4} - \frac{1}{4}(a_i \cdot n_a)(b_j \cdot n_a)$$

$$P_{+-} = \frac{1}{4} + \frac{1}{4}(a_i \cdot n_a)(b_j \cdot n_a)$$

$$P_{-+} = \frac{1}{4} + \frac{1}{4}(a_i \cdot n_a)(b_j \cdot n_a)$$

$$E(a_i, b_j) = -(a_i \cdot n_a)(b_j \cdot n_a)$$

← Could be n_b.

$$S = E(a_1, b_1) = -(a_1 \cdot n)(b_1 \cdot n) = -n_y \frac{1}{\sqrt{2}}(n_x + n_y)$$

$$-E(a_1, b_3) = +(a_1 \cdot n)(b_3 \cdot n) = +n_y \frac{1}{\sqrt{2}}(n_x - n_y)$$

$$E(a_3, b_1) = -(a_3 \cdot n)(b_1 \cdot n) = -n_x \frac{1}{\sqrt{2}}(n_x + n_y)$$

$$E(a_3, b_3) = -(a_3 \cdot n)(b_3 \cdot n) = -n_x \frac{1}{\sqrt{2}}(n_x - n_y)$$

$$S = \frac{1}{\sqrt{2}}\left(-n_y n_x - n_y^2 + n_y n_x - n_y^2 - n_x^2 - n_x n_y - n_x^2 + n_x n_y\right)$$

$$= -\frac{2}{\sqrt{2}} = \boxed{-\sqrt{2}} \quad \text{(half..)}$$

S can be used to detect eavesdropping.