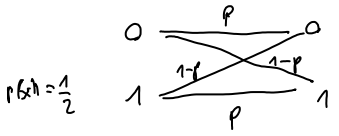
8 - Cwiczenia

18 listopada 2014
11:55

Example:

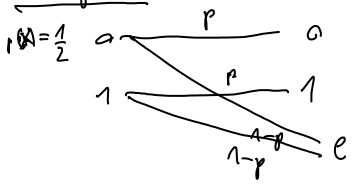


$$h(p) = -p\log_2 p - (1-p)\log_2(1-p)$$

$$I(X:Y) = 1 - h(p)$$

- $p = 100\%$ $\quad I(X:Y) = 1$
- $p = 50\%$ $\quad I(X:Y) = 0$
- for $p = 90\%$ $\quad I(X:Y) = 0{,}531$

Example:



$$H(Y) = -\frac{1}{2}p\left(\log_2\frac{p}{2} - \frac{1}{2}p\log_2\frac{p}{2} - (1-p)\log(1-p)\right)$$

$$H(Y|X) = 2\cdot\frac{1}{2}\left(-p\log p \quad - (1-p)\log(1-p)\right)$$

$$I(X:Y) = -p\log\frac{p}{2} + p\log p = p$$

Example:

Intercepted qubit attacks: r.

$$I(A:B) = 1 - h\left(\frac{r}{4}\right)$$

$$I(A:E) = r\left(1 - h(q)\right)$$

$$q = \left(\cos(22{,}5^\circ)\right)^2 = \frac{1}{4}\left(2+\sqrt{2}\right) = 0{,}146$$

$$I(A:B) = I(A:E) \Rightarrow r = 0{,}7548$$

$$\Rightarrow QBER_{th} = 18{,}9\%$$

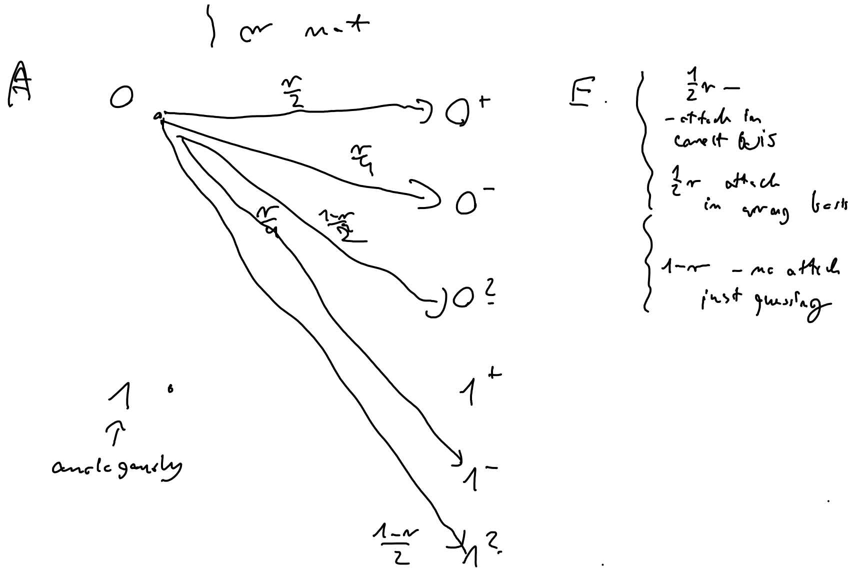
(przy użyciu bitów było 20,7% ...)

Example: Bob & Rescue, attacking a fraction r of qubits. Using random bases after $\forall$

$$QBER = \frac{r}{4} \qquad I(A:B) = 1 - h\left[\frac{r}{4}\right]$$

$I(A:E)$:

- E sees bit correctly with $p = \left(\frac{1}{2} + \frac{1}{4}\right) + (1-r)\frac{1}{2} = \frac{1}{2} + \frac{r}{4}$
- Else $e = \frac{1}{2} - \frac{r}{4}$ but he
- conclud $I(A:E) \neq 1 - h[e]$, because
- E knows whether bases were correct



$p(0^+) = \frac{r}{4}$ $p(0^-) = \frac{r}{4}$ $p(0^?) = \frac{1-r}{2}$ $p(1^+) = \frac{r}{4}$ $p(1^-) = \frac{r}{4}$ $p(1^?) = \frac{1-r}{2}$

$H(E) = -r \log \frac{r}{4} - (1-r) \log \frac{1-r}{2}$

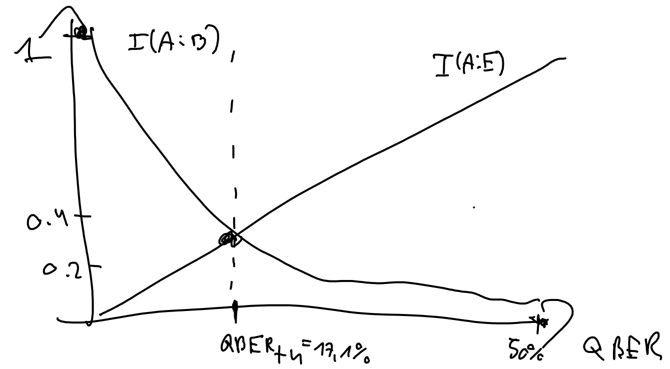
$H(E|A) = -\frac{r}{2} \log \frac{r}{2} - \frac{r}{2} \log \frac{r}{4} - (1-r) \log_2 \frac{1-r}{2}$

$H(E) - H(E|A) = \frac{r}{2} \log \frac{r}{2} - \frac{r}{2} \log \frac{r}{4} = \frac{r}{2} = I(A:E)$

For what r we will have $I(A:B) = I(A:E)$?:

$$\frac{r}{2} = 1 - h\left[\frac{r}{4}\right] \Rightarrow r = 0{,}6821$$

$QBER_{th} = 0{,}1705 \approx 17{,}1\%$



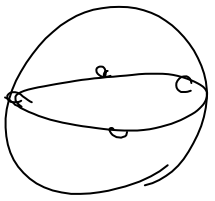
(było 25%)

Uzyskane przez informacje zmalała

Uprawdopodobnione tzg. co mymi

gorszej się o co mniej gorszym atakuj.

<u>Optimal attack on BB84:</u>



phase covariant cloning:

$$|0\rangle_A|0\rangle_E \to \sqrt{\tfrac{1}{2}}|0\rangle_B|0\rangle_E|0\rangle_X + \tfrac{1}{\sqrt{2}}(\cos\eta|0\rangle|1\rangle + \sin\eta|1\rangle|0\rangle)$$

$$|1\rangle_A|0\rangle_E|0\rangle_X \to \tfrac{1}{\sqrt{2}}(\cos\eta|1\rangle|0\rangle + \sin\eta|0\rangle|1\rangle)|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle|1\rangle|1\rangle$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi}|1\rangle)$$

$$|\psi\rangle|0\rangle|0\rangle \to \frac{1}{2}\Big(|0\rangle(|0\rangle + \cos\eta|0\rangle + \sin\eta|1\rangle) + e^{i\varphi}(|1\rangle(|1\rangle + \cos\eta|0\rangle + \sin\eta|1\rangle)\Big)$$

$$\rho_A = \frac{1}{4}\left(\begin{bmatrix}1 & \cos\eta e^{-i\varphi}\\ \cos\eta e^{i\varphi} & \cos^2\eta\end{bmatrix} + \begin{bmatrix}0 & 0\\ 0 & \sin^2\eta\end{bmatrix} + \begin{bmatrix}\sin^2\eta & 0\\ 0 & 0\end{bmatrix} + \begin{bmatrix}\cos^2\eta & \cos\eta e^{-i\varphi}\\ \cos\eta e^{i\varphi} & 1\end{bmatrix}\right) =$$

$$= \frac{1}{4}\cdot\begin{bmatrix}2 & 2\cos\eta e^{-i\varphi}\\ 2\cos\eta e^{i\varphi} & 2\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1 & \cos\eta e^{-i\varphi}\\ \cos\eta e^{i\varphi} & 1\end{bmatrix} =$$

$$= \cos\eta\,|\psi\rangle\langle\psi| + \frac{1}{2}(1-\cos\eta)\mathbb{1}$$

$$F_A = \frac{1}{2}(1+\cos\eta)$$

$$\rho_B = \frac{1}{2}\begin{bmatrix}1 & \sin\eta e^{-i\varphi}\\ \sin\eta e^{i\varphi} & 1\end{bmatrix} \qquad F_B = \frac{1}{2}[1+\sin\eta]$$

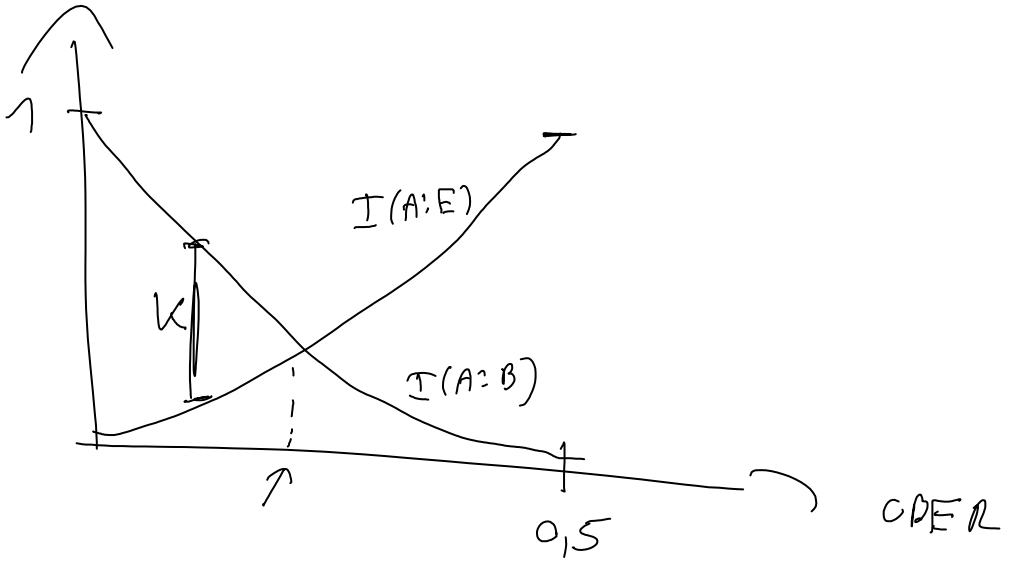
Ach nr BB84, klonowanie + pomiar w optymalnej bazie.

$$\rho_{out} = \frac{1}{2}(1-\cos\eta)$$

$QBER = \frac{1}{2}(1 - \cos\gamma)$

$e_E = \frac{1}{2}(1 - \sin\gamma)$

Klucz: $K = \cdot \left(I(A:B) - I(A:E) \right) =$



$\gamma = \frac{\pi}{4}$ $\quad QBER = \frac{1}{2}\left(1 - \frac{\sqrt{2}}{2}\right) = \frac{2-\sqrt{2}}{4} \approx 14{,}6\ \%$

Optymalny atak indywidualny.