- QKD Security definition

A, B, E $\Big\}\ \rho^{Real}_{ABE}$

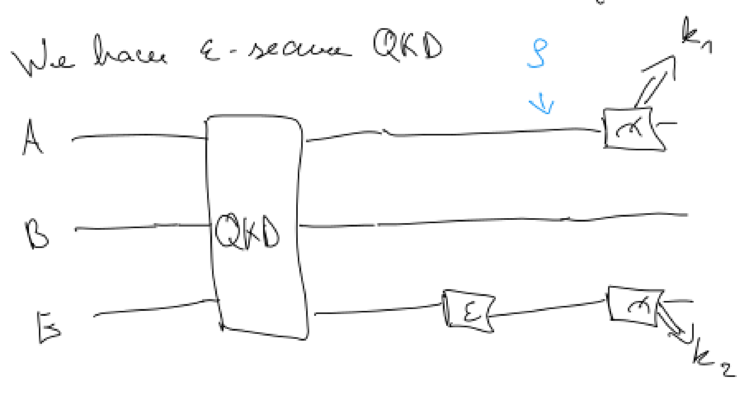
$$\rho^{Ideal}_{ABE} = \left(\sum_{k\in\{0,1\}^n} 2^{-n} |k\rangle\langle k|_A \otimes |k\rangle\langle k|_B\right)\otimes \rho_E$$

$$S_{Ideal} = \left\{\left(\sum_{k\in\{0,1\}^n} 2^{-n} |k\rangle\langle k|_A \otimes |k\rangle\langle k|_B\right)\otimes \rho_E : \rho_E \text{ is a density op}\right\}$$

Guess: $\frac{1}{2^n}$

$P_k := |k\rangle\langle k| \otimes I \otimes |k\rangle\langle k|$

We have ε-secure QKD



$$\Pr[k_1 = k_2] = \sum_k \Pr[\underset{\text{yes/no}}{k_1 = k \wedge k_2 = k}] =$$

$$= \sum_k \mathrm{tr}\, P_k \rho = \mathrm{tr}\left(\sum_k P_k\right)\rho \overset{\varepsilon}{\approx} \mathrm{tr} \sum_k P_k \rho_{ideal} =$$

$$= \mathrm{tr} \sum_{k'} |k'\rangle\langle k'| \otimes I \otimes |k'\rangle\langle k'| \sum_k 2^{-n} |k\rangle\langle k|_A \otimes |k\rangle\langle k|_B \otimes \rho_E =$$

$$= \mathrm{tr} \sum_{k,k'} 2^{-n} |k'\rangle\underbrace{\langle k'|k\rangle}_{\substack{1 \text{ if } k=k' \\ 0 \text{ otherwise}}}\langle k| \otimes |k\rangle\langle k| \otimes |k'\rangle\langle k'|\rho_E =$$

$$= \mathrm{tr}\ 2^{-n} \sum_k |k\rangle\langle k| \otimes |k\rangle\langle k| \otimes \underbrace{|k\rangle\langle k|\rho_E}_{\mathrm{tr}=?} = 2^{-n}\cdot 1 = 2^{-n}$$

Answer: $2^{-n} + \varepsilon$

Sec def w/ abort

prob p that QKD aborts. If aborts then $\rho_{abort} : |\perp\rangle\langle\perp|_A \otimes |\perp\rangle\langle\perp|_B \otimes \rho_E$

Before Sec_1 $\mathrm{TD}(\rho_{real}, \rho_{ideal}) \cdot \Pr[succ] \leq \varepsilon$ (p)

Now : Sec_2 $\mathrm{TD}(\hat\rho_{real}, \hat\rho_{ideal}) \leq \varepsilon$

includes abort

Run QKD $\rightarrow$ get ρ_{real}

$\searrow^{abort}$ ρ_{abort}

$$\tilde S_{ideal} = \left\{ p\left(\sum_k |k\rangle\langle k|_A \otimes |k\rangle\langle k|_B\right)\otimes\rho_E + (1-p)\left(|\perp\rangle\langle\perp|_A \otimes |\perp\rangle\langle\perp|_B \otimes \rho_{E\perp}\right) : \rho_E, \rho_{E\perp} \text{ are density ops}\right\}$$

$Sec_1 \Rightarrow Sec_2$

We have QKD $\rightarrow \rho_{real}$ w/ succ prob p.

$\exists \rho_{ideal}$ ε-close to ρ_{real}

$$\tilde\rho_{real} := p\,\rho_{real} + (1-p)|\perp\rangle\langle\perp| \otimes |\perp\rangle\langle\perp| \otimes \rho_{E\perp} = p\rho_{real} + \bar p \rho_{\perp R}$$

$$\hat\rho_{ideal} \in \tilde S_{ideal}$$

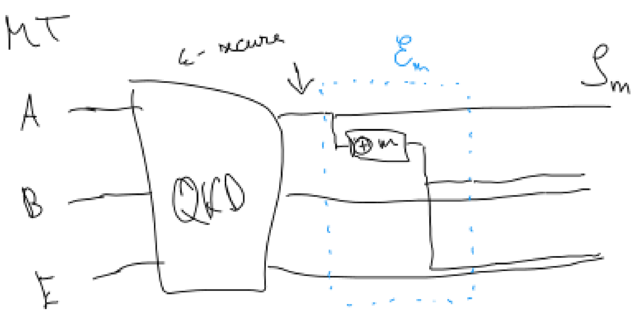
$$\hat\rho_{ideal} := p_i \rho_{ideal} + \bar p_i \rho_{\perp R}$$

assume : $p_i = p$

$$\mathrm{TD}(\tilde\rho_{real}, \hat\rho_{ideal}) = \mathrm{TD}(p\rho_{real} + \cancel{\bar p\rho_{\perp R}}, p\rho_{ideal} + \cancel{\bar p\rho_{\perp R}}) = p\cdot\mathrm{TD}(\rho_{real}, \rho_{ideal}) = \mathrm{TD}(\rho_{real}, \rho_{ideal})\cdot\Pr[succ] \leq \varepsilon$$

$Sec_2 \Rightarrow Sec_1$ left to the reader

SMT



ρ_m $\forall E\ \forall m_0, \forall m_1\ \mathrm{TD}(\mathrm{tr}_{AB}\,\rho_{m_0}, \mathrm{tr}_{AB}\,\rho_{m_1}) \leq \delta$

$$\begin{array}{ccccccc}
\rho_{real_{m_0}} & \overset{\varepsilon}{\underset{QKD}{\text{———}}} & & \rho_{ideal} & & \overset{\varepsilon}{\underset{QKD}{\text{———}}} & \rho_{real_{m_1}} \\
\Big|\,\mathcal{E}_{m_0} & & \mathcal{E}_{m_0}\,/ & & \backslash\,\mathcal{E}_{m_1} & & \Big|\,\mathcal{E}_{m_1} \\
\rho'_{real_{m_0}} & \overset{\varepsilon}{\text{———}} & \rho'_{ideal_{m_0}} & \overset{???}{\text{———}} & \rho'_{ideal_{m_1}} & \overset{\varepsilon}{\text{———}} & \rho'_{real_{m_1}} \\
\Big|\,\mathrm{tr}_{AB} & & \Big|\,\mathrm{tr}_{AB} & & \Big|\,\mathrm{tr}_{AB} & & \Big|\,\mathrm{tr}_{AB} \\
\rho''_{real_{m_0}} & \overset{\varepsilon}{\text{———}} & \rho''_{ideal_{m_0}} & \overset{\sigma = 0}{\text{———}} & \rho''_{ideal_{m_1}} & \overset{\varepsilon}{\text{———}} & \rho''_{real_{m_1}}
\end{array}$$

$\delta \leq 2\varepsilon + \sigma = 2\varepsilon$

$\mathrm{TD}(\mathcal{E}_{m_0}(\rho_{real}), \mathcal{E}_{m_0}(\rho_{ideal})) \overset{?}{\leq}$

$\mathrm{TD}(\rho_{real}, \rho_{ideal}) \leq \varepsilon$

$\mathrm{TD}(\mathcal{E}_{m_0}(\rho_{ideal}), \mathcal{E}_{m_1}(\rho_{ideal}))$ (F, G)

$$\mathcal{E}_{m_0}\Big(p\underbrace{\left(\sum_k 2^{-n}|k\rangle\langle k|_A \otimes |k\rangle\langle k|_B \otimes \rho_E\right)}_{\rho_{ideal}} + (1-p)\rho_{abort}\Big) \rightarrow p\left(\sum_k 2^{-n}|k\rangle\langle k|_A \otimes |k\oplus m_0\rangle\langle k\oplus m_0|_B \otimes |k\rangle\langle k|_B \otimes |k\oplus m_0\rangle\langle k\oplus m_0|_E \otimes \rho_E\right) + (1-p)\rho_{abort} = \rho'_{ideal_{m_0}}$$

$$\rho''_{ideal_{m_0}} = \mathrm{tr}_{AB}\,\rho'_{ideal_{m_0}} = p\left(\sum_k 2^{-n}|k\oplus m_0\rangle\langle k\oplus m_0| \otimes \rho_E\right) + (1-p)\rho_{abort_E} = \left(\sum_k 2^{-n}|k\rangle\langle k|\right)\otimes\rho_E + \bar p\,\rho_{abort_E}$$

$$\left(\sum_k 2^{-n}|k\oplus m_0\rangle\langle k\oplus m_0|\right)\otimes\rho_E =$$

$$= \left(\sum_k 2^{-n}|k\rangle\langle k|\right)\otimes\rho_E$$

Doesn't depend on m_0, m_1

$\mathrm{TD}(\rho''_{ideal_{m_0}}, \rho''_{ideal_{m_1}}) = 0 = \sigma$

$$\beta_{00} = \frac{1}{\sqrt2}|00\rangle + \frac{1}{\sqrt2}|11\rangle$$

$$(H\otimes H)\beta_{00} = \frac{1}{\sqrt2}|+\rangle\otimes|+\rangle + \frac{1}{\sqrt2}|-\rangle\otimes|-\rangle = \frac{1}{\sqrt2}\left(\underbrace{\frac{1}{\sqrt2}(|0\rangle \pm |1\rangle)\otimes\frac{1}{\sqrt2}(|0\rangle \pm |1\rangle)}\right) + \ \dots\dots \quad = \beta_{00}$$

$$\frac12|00\rangle + \cancel{\frac12|01\rangle} + \cancel{\frac12|10\rangle} + \frac12|11\rangle$$

$$\frac12|00\rangle - \cancel{\frac12|01\rangle} - \cancel{\frac12|10\rangle} + \frac12|11\rangle$$

$(U\otimes U)\beta_{00} = \beta_{00}$ if U is real