$\forall \tilde{S}_{real}\ \forall E\ \exists S_{ideal} \in S^{ideal}:\ TD(S_{real}, S_{ideal}) \cdot P_r[\text{success}] \le \varepsilon$

Sec 1 (§3) / Sec 2

$\tilde{S}_{real}\ \forall E\ \exists \tilde{S}_{ideal} \in \tilde{S}^{ideal}: TD(\tilde{S}_{real}, \tilde{S}_{ideal}) \ge \varepsilon$

$\tilde{S}_{real} = p\, S_{real} + \bar{p}\, S_{abort}$

$Sec_1 \Rightarrow Sec_2$ (work lab)

$Sec_2 \Rightarrow Sec_1$ (reuse)

Have: $\tilde{S}_{real}\ \exists \tilde{S}_{ideal}\ TD(\tilde{S}_{real}, \tilde{S}_{ideal}) \le \varepsilon$

Want $TD(S_{real}, S_{ideal}) \cdot P_r[succ] \le \varepsilon$

$S_{real} = \frac{\tilde{S}_{real} - \bar{p}\tilde{S}_{abort}}{p}$ because p is same in real and ideal

$S_{ideal} = \frac{\tilde{S}_{ideal} - \bar{p}\tilde{S}_{abort}}{p}$

$Sec_1 = TD(S_{real}, S_{ideal}) \cdot p = TD\left(\frac{\tilde{S}_{real} - \bar{p}\tilde{S}_{abort}}{p}, \frac{\tilde{S}_{ideal} - \bar{p}\tilde{S}_{abort}}{p}\right) \cdot p = TD(\tilde{S}_{real} - \bar{p}\tilde{S}_{abort}, \tilde{S}_{ideal} - \bar{p}\tilde{S}_{abort}) =$

$= TD(\tilde{S}_{real}, \tilde{S}_{ideal}) \le \varepsilon$

$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ → ✓

$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$ → X

$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$ → Z

$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$ → ZX

$|\beta_{00}\rangle \otimes |\beta_{00}\rangle$

$|\widetilde{xy}\rangle = |\beta_{x_1y_1}\rangle \otimes |\beta_{x_2y_2}\rangle \otimes \dots$

$|\widetilde{0000}\rangle = |\beta_{00}\rangle \otimes |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) =$

$= \frac{1}{2}|0000\rangle + \frac{1}{2}|0011\rangle + \frac{1}{2}|1100\rangle + \frac{1}{2}|1111\rangle \rightsquigarrow$

$\rightsquigarrow \frac{1}{2}|0000\rangle + \frac{1}{2}|0101\rangle + \frac{1}{2}|1010\rangle + \frac{1}{2}|1111\rangle =$

$= \sum_{k \in \{0,1\}^4} \frac{1}{2}|k\rangle \otimes |k\rangle$

$|\beta_{ij}\rangle = \underbrace{(I \otimes (X^i Z^j))}_{U^{ij}} |\beta_{00}\rangle = (I \otimes U^{ij})|\beta_{00}\rangle$

$|xy| := |\{i : x_i y_i \neq 00\}|$

0	00
1	00
2	11
3	00

$|00\rangle\langle 10|\otimes|00\rangle\langle 00| = 2$

$\sum_{|xy| \le t} \lambda_{xy} |\widetilde{xy}\rangle \otimes |\psi_{E_{xy}}\rangle$

Can Eve guess the key if errors are introduced

First: No errors, $|\psi\rangle = |\widetilde{00\dots0}\rangle \otimes |\psi_E\rangle$

$P_r[K_A = K_E] = \sum_k P_r[K_A = k \wedge K_E = k] = \sum_k \|P_k|\psi\rangle\|^2$

$P_k = |kk\rangle\langle kk| \otimes I \otimes |kk\rangle\langle kk|$

$\sum_k \|P_k\, 2^{\frac{n}{2}} \sum_z |z\rangle \otimes |z\rangle \otimes |\psi_z\rangle_E\| = \sum_k \| 2^{\frac{n}{2}} \sum_z |kk\rangle\langle zz| \otimes |z\rangle \otimes |kk\rangle\langle kk|\psi_E\rangle \|^2 =$

$\sum_k \| 2^{\frac{n}{2}} |k\rangle \otimes |k\rangle \otimes |kk\rangle\langle kk|\psi_E\rangle\|^2 = \frac{1}{2^n} \sum_k \| |k\rangle \otimes |k\rangle \otimes |kk\rangle\langle kk|\psi_E\rangle\|^2 = \frac{1}{2^n} \cdot 1 = \frac{1}{2^n}$

$|\psi_E\rangle = \sum_k \alpha_k |k\rangle \quad \sum_k |\alpha_k|^2 = 1$

With errors: $|\psi\rangle = \sum_{|xy| \le t} \lambda_{xy} |\widetilde{xy}\rangle \otimes |\psi_{E_{xy}}\rangle$

$\sum_i \|\alpha_i \psi_i\|^2 \le \left(\sum_i |\alpha_i|^2\right)\left(\sum_i \|\psi_i\|^2\right)$

$\sum_k P_r[K_A = k \wedge K_E = k] = \sum_k \| \sum_{|xy| \le t} \lambda_{xy} P_k(|\widetilde{xy}\rangle \otimes |\psi_{E_{xy}}\rangle) \|^2 \le \sum_k \left(\sum_{|xy| \le t} |\lambda_{xy}|^2\right)\left(\sum_{|xy| \le t} \|P_k(|\widetilde{xy}\rangle \otimes |\psi_{E_{xy}}\rangle)\|^2\right) =$

$= \sum_{|xy| \le t} \sum_k \|P_k(|\widetilde{xy}\rangle \otimes |\psi_{E_{xy}}\rangle)\|^2 = \sum_{|xy| \le t} \sum_k \|P_k\left(2^{\frac{n}{2}} \sum_z |z\rangle \otimes U^{xy}|z\rangle \otimes |\psi_{E_{xy}}\rangle\right)\|^2 =$

$= \sum_{|xy| \le t} \sum_k 2^n \left\| \sum_z |kk\rangle\langle zz| U^{xy}|z\rangle \otimes |kk\rangle\langle kk|\psi_{E_{xy}}\rangle \right\|^2 =$

$= \sum_{|xy| \le t} 2^n \left(\sum_k \left\| |k\rangle \otimes U^{xy}|k\rangle \otimes |kk\rangle\langle kk|\psi_{E_{xy}}\rangle \right\|^2 \right) =$

$= \sum_{|xy| \le t} 2^{-n} \cdot 1 = \frac{|M|}{2^n} \quad \{xy : |xy| \le t\}$

$(I \otimes U)|00\dots0\rangle = (I \otimes U)\left(2^{-\frac{n}{2}} \sum_k |k\rangle \otimes |k\rangle\right) = 2^{-\frac{n}{2}} \sum_k |k\rangle \otimes U|k\rangle$

QKD last step drop last bit of key

Basic idea: Trace away last bit, we security of n-1 bit key

QKD last not last bit of key to 0

last bit always 0

$S_{real}\ \exists S_{ideal}\ TD(S_{real}, S_{ideal}) \cdot P_r[succ] \le \varepsilon$ ($\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle$)

$\le TD(\mathcal{E}(S_{real})\ \mathcal{E}(S_{ideal})) \le$

$\le TD(|0\rangle\langle 0|, I)$ ← large