

Individual attack

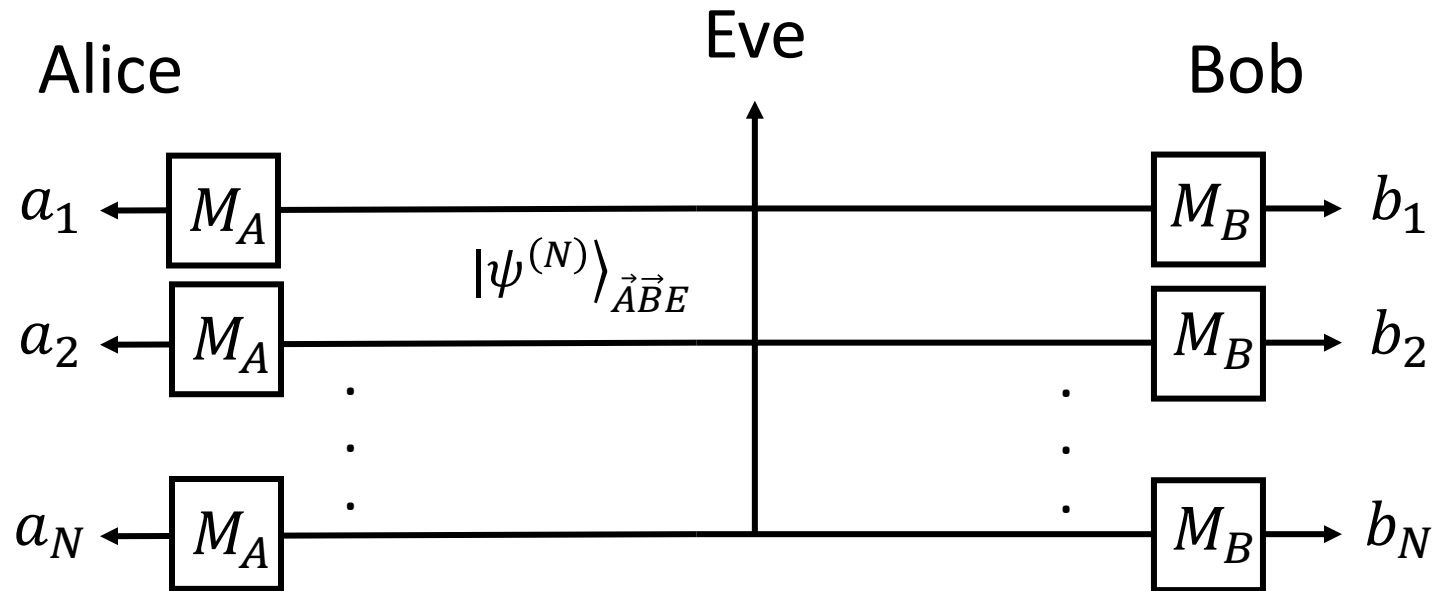
$$P(\vec{a}, \vec{b}, \vec{e}) = P(a, b, e)^{\times N}$$

$$P(a, b, e) = \langle \psi | M_A \otimes M_B \otimes M_E | \psi \rangle$$

Collective attack

$$\rho_{\vec{A}\vec{B}\vec{E}} = \rho_{ABE}^{\otimes N}$$

$$\rho_{ABE} = \sum_{a,b} P(a, b) |ab\rangle\langle ab| \otimes |e^{ab}\rangle\langle e^{ab}|$$



General attack

$$\rho_{\vec{A}\vec{B}\vec{E}}^{(N)} = \sum_{\vec{a}, \vec{b}} P(\vec{a}, \vec{b}) |\vec{a}\vec{b}\rangle\langle \vec{a}\vec{b}| \otimes |e^{\vec{a}, \vec{b}}\rangle\langle e^{\vec{a}, \vec{b}}|$$