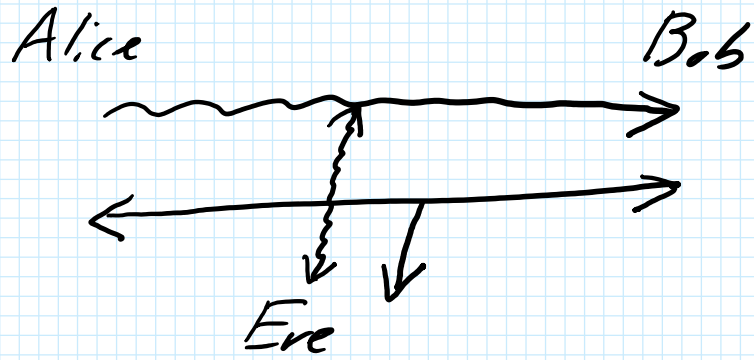

- prepare-and-measure (BB84)
- entanglement-based (Ekert 91)

Protocol:

① Distribution

for $i=1,\dots N$:

A	B
- prepares state $\phi^+ = \lvert 0\rangle_A\lvert 0\rangle_B + \lvert 1\rangle_A\lvert 1\rangle_B$	—
- sends B-part to Bob	—
- choose a random bit $T_i \in \{0,1\}$	- choose a random bit $T_i' \in \{0,1\}$
- measurement of A in basis $\{\lvert 0\rangle, \lvert 1\rangle\}$ if $T_i=0$, $\{\lvert 0\rangle, \lvert 1\rangle\}$ if $T_i=1$	meas of B: " " $T_i'=0$, " " $T_i'=1$

② Sifting

Discard positions where $T_i \neq T_i'$

Let $X=(X_1,\dots X_n)$ be the remaining outcomes of meas.

Let $Y=(Y_1,\dots Y_n)$ " "

③ Verification

repeat t_n times { Alice chooses some indices i at random and reveals (i, X_i)

Bob compares X_i and Y_i

If disagreement, he notifies Alice and they abort the protocol.

④ Privacy amplification

output the non-revealed pos. of X as key S_A

outputs "" of Y as key S_B.

Claim: Either

- protocol aborts
- generates key and key is secure

} with prob. $\geq 1-\varepsilon$, $\varepsilon \simeq 10^{-7}$

Notation:

$\phi^+ = |00\rangle + |11\rangle = |\bar{0}\bar{0}\rangle + |\bar{1}\bar{1}\rangle$

$\phi^- = |00\rangle - |11\rangle = |\bar{0}\bar{1}\rangle + |\bar{1}\bar{0}\rangle$ ←

$\psi^+ = |01\rangle + |10\rangle = |\bar{0}\bar{0}\rangle - |\bar{1}\bar{1}\rangle$

$\psi^- = |01\rangle - |10\rangle = |\bar{1}\bar{0}\rangle - |\bar{0}\bar{1}\rangle$ ←

Note: $\mathrm{span}\{\phi^-, \psi^-\} = \mathrm{span}\{|\bar{0}\bar{1}\rangle, |\bar{1}\bar{0}\rangle\}$

$\mathrm{span}\{\psi^+, \psi^-\} = \mathrm{span}\{|01\rangle, |10\rangle\}$ } ⊗

Assumption:

State of Alice and Bob before meas.

$\int A_1 B_1 \dots A_n B_n = \sigma_{AB}^{\otimes N}$ for σ_{AB} arbitrary

$\rho_{A_1B_1 \ldots A_nB_n} = \sigma_{AB}^{\otimes n}$ for σ_{AB} arbitrary

Verification is equivalent to check that

$\langle 01 | \sigma_{AB} | 01 \rangle \approx 0$

$\langle 10 | \sigma_{AB} | 10 \rangle \approx 0$

$\langle 0\bar{1} | \sigma_{AB} | 0\bar{1} \rangle \approx 0$

$\langle \bar{1}0 | \sigma_{AB} | \bar{1}0 \rangle \approx 0$

(provided test is successful, i.e. don't abort)

(*) $\langle \psi^+ | \sigma_{AB} | \psi^+ \rangle \approx 0$

$\langle \phi^- | \sigma_{AB} | \phi^- \rangle \approx 0$

$\langle \psi^- | \sigma_{AB} | \psi^- \rangle \approx 0$

$\Rightarrow \sigma_{AB} \approx |\phi^+\rangle\langle\phi^+|$

Let σ_{ABE} the state describing also Eve's information.

Condition $\sigma_{AB} = \mathrm{tr}_E(\sigma_{ABE})$

Because σ_{AB} is pure it follows that

$\sigma_{ABE} \approx \sigma_{AB} \otimes \sigma_E$, i.e.,

E is independent of AB.

Because the keys S_A and S_B are obtained from measurements on AB, they are also independent of E and therefore secret!