Quantum key distribution

Idea (roughly): Alice and Bob share

N Bell-pairs $|\mathcal{B}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$,

$$|\psi_{AB}\rangle = |\mathcal{B}\rangle^{\otimes N};$$

- Alice measures $Q = |1\rangle\langle 1|_A^{\otimes N}$
- Bob measures $S = |1\rangle\langle 1|_B^{\otimes N}$

→ identical <u>random</u> sequences, e.g.

$$q_N = (001 \dots 1011)$$

$$s_N = (001 \dots 1011)$$

which may be use as cryptographic keys.

⚠ eavesdropper Eve could measure

Q or S before!

→ on a random fraction of their

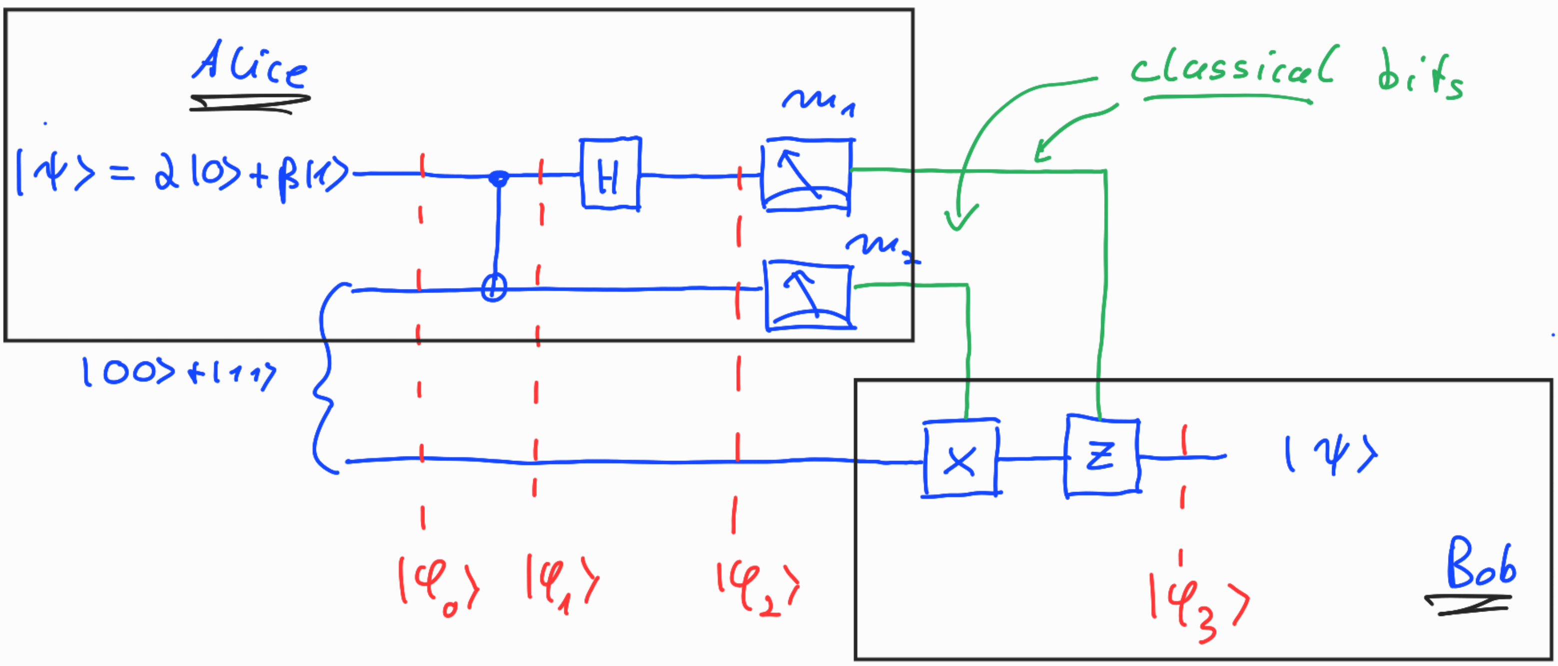
Bell-pairs, Alice and Bob

should check entanglement by e.g. testing CHSH-inequality!

Quantum - teleportation:

a shared Bell-pair can be use to transfer one qubit by the transmission of two classical bits:

Protocoll:



$$|\varphi_0\rangle = (\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle)/\sqrt{2}$$

$$|\varphi_1\rangle = \alpha|0\rangle(|00\rangle + |11\rangle)/\sqrt{2} + \beta|1\rangle(|10\rangle + |01\rangle)/\sqrt{2}$$

$$\rightarrow 2|\varphi_2\rangle = \alpha\,(|0\rangle+|1\rangle)(|00\rangle+|11\rangle) + \beta\,(|0\rangle-|1\rangle)(|10\rangle+|01\rangle)$$

$$
\begin{array}{lcccccc}
 & & m_1\ m_2 & : & & & |\varphi_3\rangle \\
\overset{!}{=} |00\rangle(\alpha|0\rangle+\beta|1\rangle) & : & 0\ \ 0 & : & I & : & |\psi\rangle \\
+\,|01\rangle(\alpha|1\rangle+\beta|0\rangle) & : & 0\ \ 1 & : & X & : & |\psi\rangle \\
+\,|10\rangle(\alpha|0\rangle-\beta|1\rangle) & : & 1\ \ 0 & : & Z & : & |\psi\rangle \\
+\,\underbrace{|11\rangle}_{\text{measurement}}(\alpha|1\rangle-\beta|0\rangle) & : & 1\ \ 1 & : & XZ & : & |\psi\rangle
\end{array}
$$

✓

Distillation of entanglement

Alice and Bob share a general composed system AB in an entangled (pure!) state $|\psi_{AB}\rangle$. Exclusively by local operations and classical communication (LOCC) they want to convert the entanglement of AB into the entanglement of Bell-pairs ($|00\rangle \pm |11\rangle$, $|01\rangle \pm |10\rangle$).

How many Bell-pairs can be "distilled" in this way from $|\psi_{AB}\rangle$?

<u>Thm.</u>: <u>Entanglement distillation</u>

From N copies of $|\psi_{AB}\rangle$, $K = N\, S(\rho_A)$ Bell-pairs can be distilled by local operations and classical communication.

$\rightarrow$ von Neumann entropy $S(\rho_A)$ of the reduced state $\rho_A = \mathrm{tr}_B\, |\psi_{AB}\rangle\langle\psi_{AB}|$ <u>measures</u> entanglement of $|\psi_{AB}\rangle$ in <u>units of Bell-pairs</u>!

<u>Proof</u>

(I) Schmidt decomposition of K Bell pairs

$|\beta\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$:

with $|\tilde{0}\rangle = |00\rangle$, $|\tilde{1}\rangle = |11\rangle$

$$|\tilde{i}\rangle_{AB} = |\tilde{i}_{k-1}\rangle\, |\tilde{i}_{k-2}\rangle \cdots |\tilde{i}_0\rangle$$

$$= |i_{k-1}\rangle_A\, |i_{k-2}\rangle_A \cdots |i_0\rangle_A \otimes$$

$$|i_{k-1}\rangle_B\, |i_{k-2}\rangle_B \cdots |i_0\rangle_B$$

$$= |i\rangle_A \otimes |i_B\rangle \qquad (0 \leq i \leq 2^k)$$

: $$|\ell\rangle^{\otimes k} = \left(\frac{|\tilde{0}\rangle + |\tilde{1}\rangle}{\sqrt{2}}\right)^{\otimes k} = 2^{-k/2} \sum_{i=0}^{2^k-1} |\tilde{i}\rangle_{AB}$$

$$= 2^{-k/2} \sum_{i=0}^{2^k-1} |i\rangle_A \otimes |i\rangle_B \, .$$

(II) Schmidt decomposition of $|\psi_{AB}\rangle$:

$$|\psi_{AB}\rangle = \sum_{j=0}^{d-1} \sqrt{p_j}\, |\varphi_j\rangle_A\, |\chi_j\rangle_B$$

$$\rightsquigarrow \quad \rho_A = \sum p_j\, |\varphi_j\rangle\langle\varphi_j|$$

$$\rho_B = \sum p_j\, |\chi_j\rangle\langle\chi_j|$$

$$\rightsquigarrow \quad |\psi_{AB}\rangle^{\otimes N} = \sum_{\underline{j}=0}^{d^N-1} \sqrt{p_{\underline{j}}}\, |\varphi_{\underline{j}}\rangle |\chi_{\underline{j}}\rangle$$

- $$p_{\underline{j}} = \prod_{\ell=0}^{N-1} p_{j_\ell}$$
- $$|\varphi_{\underline{j}}\rangle = \bigotimes_{\ell=0}^{N-1} |\varphi_{j_\ell}\rangle$$
- $$|\chi_{\underline{j}}\rangle = \bigotimes_{\ell=0}^{N-1} |\chi_{j_\ell}\rangle$$

$$\rightarrow \quad \rho_A^{\otimes N} = \operatorname{tr}_{B^N} |\psi_{AB}\rangle\langle\psi_{AB}|^{\otimes N}$$

$$= \sum_{\underline{j}=0}^{d^N-1} p_{\underline{j}}\, |\varphi_{\underline{j}}\rangle\langle\varphi_{\underline{j}}|$$

$$\rho_B^{\otimes N} = \sum_{\underline{j}=0}^{d^N-1} p_{\underline{j}}\, |\chi_{\underline{j}}\rangle\langle\chi_{\underline{j}}|$$

$\rightarrow$ typical subspaces:

$$T_A = \operatorname{Span}\left\{ |\varphi_{\underline{j}}\rangle \;\middle|\; p_{\underline{j}} =_\varepsilon 2^{-N\cdot S} \right\}$$

$$T_B = \operatorname{Span}\left\{ |\chi_{\underline{j}}\rangle \;\middle|\; p_{\underline{j}} =_\varepsilon 2^{-N\cdot S} \right\}$$

where $S = S(\rho_A) = S(\rho_B)$

since $\dim T_{A/B} =_\varepsilon 2^{-K}$, $K = N \cdot S$, the following distillation protocols work:

<u>Alice</u>: (1) projection P_A on T_A

(2) unitary encod. $U_A : T_A \to \mathcal{H}_k^A$

$$|\varphi_j\rangle \mapsto |i_j\rangle_A$$

<u>Bob</u>: (1) projection P_B on T_B

(2) unitary encod. $U_B : T_B \to \mathcal{H}_K^B$

$$|\chi_j\rangle \mapsto |i_j\rangle_B$$

<u>Check</u>:

$$(U_A P_A \otimes 1\!\!1_B)(1\!\!1_A \otimes U_B P_B) \, |\psi_{AB}\rangle^{\otimes N}$$

$$= (U_A \otimes U_B)(P_A \otimes P_B) \sum_{j=0}^{d^N-1} \mu_j^{1/2} \, |\varphi_j\rangle |\chi_j\rangle$$

$$= U_A \otimes U_B \sum_{\substack{j: \\ \mu_j =_\varepsilon 2^{-K}}} 2^{-K/2} \, |\varphi_j\rangle |\chi_j\rangle$$

$$= \sum_{\substack{j: \\ \mu_j =_\varepsilon 2^{-K}}} 2^{-K/2} \, |i_j\rangle_A \, |i_j\rangle_B = 2^{-K/2} \sum_{i=0}^{2^k-1} |i\rangle_A |i\rangle_B$$

$$= |\ell\rangle^{\otimes k}$$

■

Average entanglement of random states

(D. P. Page, 1993)

What is the average entanglement

$S = \overline{S(\rho_A)}$ of a random (w.r.t. unitarily inv. meas.) pure state

$|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$?

for large dimensions $D_B \gg D_A \gg 1$:

$$\boxed{S \simeq \log D_A}$$

$$\to \quad \rho_A \simeq \mathbb{1}_A / D_A$$

→ random pure states are almost always nearly maximally entangled !

To show this it is convenient to use

Rényi - entropies (quantum version) :

$$S_\alpha(\rho) := \frac{1}{1-\alpha} \log_2 \operatorname{tr} \rho^\alpha \, ; \qquad \alpha \in \,]0,\infty[\, \setminus \{1\}$$

two facts: (i) $\lim_{\alpha \to 1} S_\alpha(\rho) = S(\rho)$

$\uparrow$ von Neumann entr.

(ii) $\frac{\partial S_\alpha}{\partial \alpha} \leq 0 \, !$ $\rightsquigarrow$ $S_\alpha(\rho) \leq S_\beta(\rho)$ for $\alpha \geq \beta$

(i) and (ii) yield $S_2(\rho) = -\log_2 \operatorname{tr} \rho^2$ as an easily computable lower bound for $S(\rho)$!

<u>Note</u>: For $\rho = P/d$, where P projection of rank d, <u>purity</u> $\operatorname{tr} \rho^2 = \operatorname{tr} P/d^2 = 1/d$

$\rightsquigarrow$ $S_2(\rho) = \log_2 d = S(\rho)$

to compute $\overline{\operatorname{tr} \rho_A^2}$ we expand

$$|\psi_{AB}\rangle = \sum_{i=1}^{D_A} \sum_{\ell=1}^{D_B} u_{i\ell} \, |i\rangle_A \, |\ell\rangle_B$$

and use $\overline{|u_{il}|^2} = \frac{1}{D_A D_B}$

(by normalization of $|\psi_{AB}\rangle$).

$\rightarrow \rho_A = \mathrm{tr}_B |\psi_{AB}\rangle\langle\psi_{AB}| = \sum_{ij} \sum_{l} u_{il} u_{jl}^* |i\rangle\langle j|$

$\rightarrow \mathrm{tr}\, \rho_A^2 = \sum_{ij} \sum_{lm} u_{il} u_{jl}^* u_{jm} u_{im}^*$

$$\rightarrow \overline{\mathrm{tr}\, \rho_A^2} = \sum_{ij} \sum_{lm} \overline{u_{il} u_{jl}^* u_{jm} u_{im}^*}$$

δ_{lm} δ_{ij}

$$= \underbrace{\sum_{ij}^{D_A} \sum_{l}^{D_B}}_{D_A^2 D_B} \underbrace{\overline{|u|^4}}_{\frac{1}{D_A^2 D_B^2}} + \underbrace{\sum_{i}^{D_A} \sum_{lm}^{D_B}}_{D_A D_B^2} \underbrace{\overline{|u|^4}}_{\frac{1}{D_A^2 D_B^2}}$$

$$= \frac{1}{D_B} + \frac{1}{D_A} \underset{D_B \gg D_A}{\simeq} \frac{1}{D_A}.$$

$$\rightarrow \overline{S}(\rho_A) \geq \overline{S_2(\rho_A)} = \log D_A$$

Assuming that "random" states are reasonable representatives of actual states in real systems, entanglement appears to be an <u>omnipresent</u> quantum phenomenon; – also in our macroscopic, "classical" world?

In fact, an entangled pure state $|\psi_{AB}\rangle$ of a (microscopic) system A with its macroscopic environment B generally leads to a <u>mixed</u> reduced state $\rho_A = \mathrm{tr}_B |\psi_{AB}\rangle\langle\psi_{AB}|$, in which superpositions <u>effectively</u> have <u>collapsed</u> into their components → <u>classical behaviour due to entanglement</u>!

⇝ "<u>Decoherence</u>"

cf. "Decoherence and the Appearance of a Classical World in Quantum Theory" by Joos, Zeh, Kiefer, Giulini, Kupsch, and Stamatescu (Springer 2003)

When states $|\psi_{AB}\rangle$ of an compound system AB are typically highly entangled, why it is so difficult to establish entanglement between two microscopic systems (e.g. spins) in a distance (Bell-pairs!)?

Precisely the tendency to high entanglement of AB with a third party, an environment C, makes entanglement of A and B difficult:

for $D_C \gg D_A \cdot D_B$ random $|\psi_{ABC}\rangle$ typically exhibits almost maximal $(AB) - C$ entanglement, meaning that $S(\rho_{AB}) \simeq \log D_A D_B$ and thus

$$\rho_{AB} \simeq \frac{\mathbb{1}_{AB}}{D_A D_B} \overset{!}{=} \frac{\mathbb{1}_A}{D_A} \otimes \frac{\mathbb{1}_B}{D_B}$$

separable mixed (!) state of A and B!

(cf. "Monogamy of Entanglement")