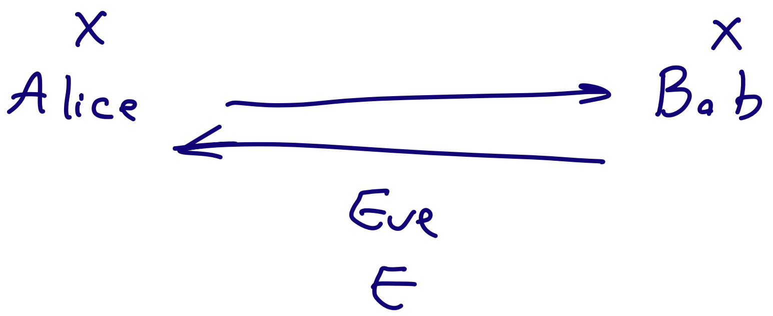
Lec 9: Random extractors

Obtaining good randomness from weak randomness

X weak randomness (low entropy) / it is correlated with another classical or quantum

Goal: obtain Y uniform & ind of E (minimal assumption)



$X \sim [N]$

$\mathrm{Ext}: [N] \to [M]$ ε-extractor

if $\| \mathrm{Ext}(X) - P_{unif} \|_1 \leq \varepsilon$

$H(X) \geq k \implies ?$

Example: $X = \begin{cases} \text{uniform } n \text{ bit} & \text{with prob } 1/2 \\ \text{constant} & \text{" " } 1/2 \end{cases}$

$H(X) = \Omega(n)$ but you cannot extract randomness

$\forall N \quad \forall k \quad \forall \varepsilon \quad X$ k-source

$m = k - 2\log(1/\varepsilon) - O(1)$ $\quad \mathrm{Ext} : [N] \to [M]$ random

$$\Pr_{\mathrm{Ext}}\left[\| \mathrm{Ext}(X) - P_{\mathrm{unif}} \|_1 \geq \varepsilon \right] \leq 2^{-\Omega(k\varepsilon^2)}$$

$\forall$ k-source $\exists$ Ext $\longrightarrow$ ε-extractor

$\exists$ extractor $\forall$?

$\forall$ $\mathrm{Ext} : [N] \to \{0,1\}$ $\exists$ $(n-1)$ source X

s.t.

seeded extractor

$\mathrm{Ext} : [N] \times [D] \longrightarrow [M]$ seeded extractor

(k,ε) - extractor if $\mathrm{Ext}(X, U_d) \approx_\varepsilon$ unif