

Krautová kryptografie

alice



Bob



Eve is an eavesdropper

Informace : 0, 1

$$\rightarrow ; |H\rangle \sim 0$$

$$\uparrow ; |V\rangle \sim 1$$

Pokud Eve očekává výstup 0

A a B mě měří

A a B používají výstup

$|D\rangle$

$|A\rangle$

$$|D\rangle = \frac{1}{\sqrt{2}} (|H\rangle + |V\rangle)$$

$$|A\rangle = \frac{1}{\sqrt{2}} (|V\rangle - |H\rangle)$$

Eve očekává 0, dostane 00/00 výsledky

$|H\rangle, |V\rangle$ a počle že dal $\rightarrow A, B$ dostanou 00.

! Trick → samciček až Ž nemůže rafabě říci měřit!

Protocol

① Alice posílá $\begin{pmatrix} 0,1 \\ \alpha \end{pmatrix}$ na hodnotu řešenou

② Bob přijima a na hodnotu měří $\alpha \rightarrow , \downarrow$

③ Po vysílání si A a B srovnají a B mahláčí, ne kterých basich měříl. A mahláčí, když to souhlasí. Kromě se budou pouze případky, když to souhlasí.

④ Bob svolá podkrevničku dat a ohláší hodnoty - pokud řešenice neobrazují čísla \Rightarrow všechny informace & později falešný Alice.