

Krautova' šifrování

Alice



Bob



Eve is an eavesdropper

Informace : 0, 1


→ i |H> ~ 0

↑ j |V> ~ 1

Pokud Eve odposlouchá v té stejné bázi

A a B nic neví

A a B používají bázi

Two arrows pointing from the text to the labels |D> and |A>.

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

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

Eve odposlouchá, dostane 0/0 výsledky

|H>, |V> a poté jí dál → A, B dostávají šifru.

