2) Quantum cryptography protocol BB84

a) Alice generates

$a = 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0.$

$b = X\ Z\ X\ X\ Z\ Z\ X\ Z\ X\ X\ X\ Z$

describe the qubits sent to Bob

$$\Rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \dots \otimes |0\rangle$$

b) Adversary Eve measures along

$b'' = Z\ X\ X\ Z\ Z\ X\ Z\ X\ Z\ Z\ X\ X$

mark the qubits which she disturbes

c) Bob measures along

$b' = Z\ X\ X\ X\ Z\ X\ Z\ Z\ Z\ X\ Z\ Z$

mark the qubits which he measured so that $b'_i = b_i$

d) Alice and Bob now should share a substring of a unless there was noise / Eve on the channel

Alice and Bob compare some random bits from their "shared substring"

- little or no disturbance detected ⇒ OK ✓ — get rid of the noise and amplify privacy
- disturbance high
  - channel is useless
  - EVE is there

⇓ cancel communication

(if Eve was there she knows irrelevant "fragments")