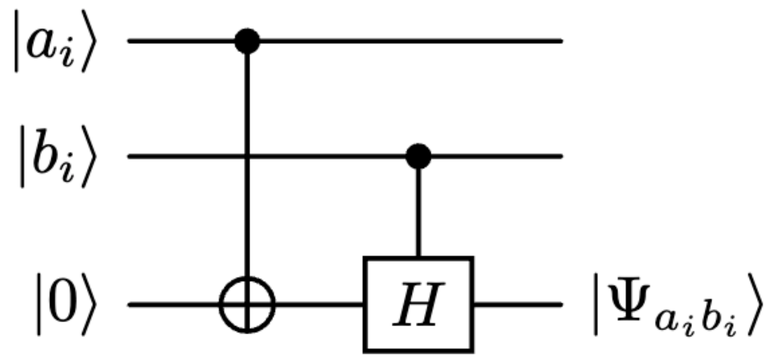
Établissement de clé quantique BB84

Préparation

- Alice génère deux chaines de n bits aléatoires a et b et les encode dans l'état de n qubits $|\Psi\rangle$

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle \quad \text{avec} \begin{cases} |\Psi_{00}\rangle = |0\rangle \\ |\Psi_{01}\rangle = |+\rangle \\ |\Psi_{10}\rangle = |1\rangle \\ |\Psi_{11}\rangle = |-\rangle \end{cases}$$



- Chaque qubit correspond au bit a_i dans la base b_i (la base de calcul ou la base de Hadamard)

Établissement de clé quantique BB84

Mesure

- Alice envoie l'état $|\Psi\rangle$ à Bob
- Bob génère une chaine de n bits aléatoires b'
- Bob mesure chaque qubit dans la base b'_i et obtient un bit a'_i