Fontys Hogescholen DE HAAGSE HOGESCHOOL Hogeschool van Amsterdam SAXION

# Introduction into Quantum Computing
# Quantum Key Distribution

During this lesson on QKD you learned how the BB84 protocol works. Make an implementation of this protocol using Qiskit. Your implementation must cover all the steps discussed during the lesson:

1. Alice randomly chooses a basis $B_i \in \{X, Z\}$ and a bit $b_i \in \{0, 1\}$.
2. Alice prepares a qubit $|q_i\rangle$ according to:

| $B_i$ | $b_i$ | $\|\psi_i\rangle$ |
|---|---|---|
| $Z$ | $0$ | $\|0\rangle$ |
| $Z$ | $1$ | $\|1\rangle$ |
| $X$ | $0$ | $\|+\rangle$ |
| $X$ | $1$ | $\|-\rangle$ |

3. Alice sends the resulting qubit $|q_i\rangle$ to Bob.
4. Bob measures the qubit $|q_i\rangle$ in a basis $\widetilde{B_i} \in \{X, Z\}$ that he picks randomly. He privately records the measurement outcome $m_i$.
5. Alice and Bob repeat the previous steps (1–4) a large number of times (N).
6. Alice and Bob publicly announce the $N$ bases they have each used.
7. Alice and Bob keep the elements in which they used the same basis ($B_i = \widetilde{B_i}$) and throw away the rest.
8. Alice and Bob randomly pick a subset of the remaining pairs $(b_i, m_i)$ and compare them. If they are equal, then they can confidently use the remaining ones as their shared key.

As mentioned before, your implementation should cover all these steps. Be sure of testing it for the following possibilities:

- *Safe scenario:* Alice and Bob are working on a clean and safe scenario. No threats are present and everything should work as expected.
- *Dangerous scenario:* A highly skilled hacker was able to break into your system and is trying to access your private key, disturbing the protocol. Can you detect her? What is the minimum number of bits that you need to compare in order to detect the hacker at your first attempt?
- *Living on the edge scenario:* Assume that, by external reasons, you can only check 6 bits (during the 8th. step of the protocol). Can you find a situation in which the hacker's interference was not detected? How long did it take you to find such situation?