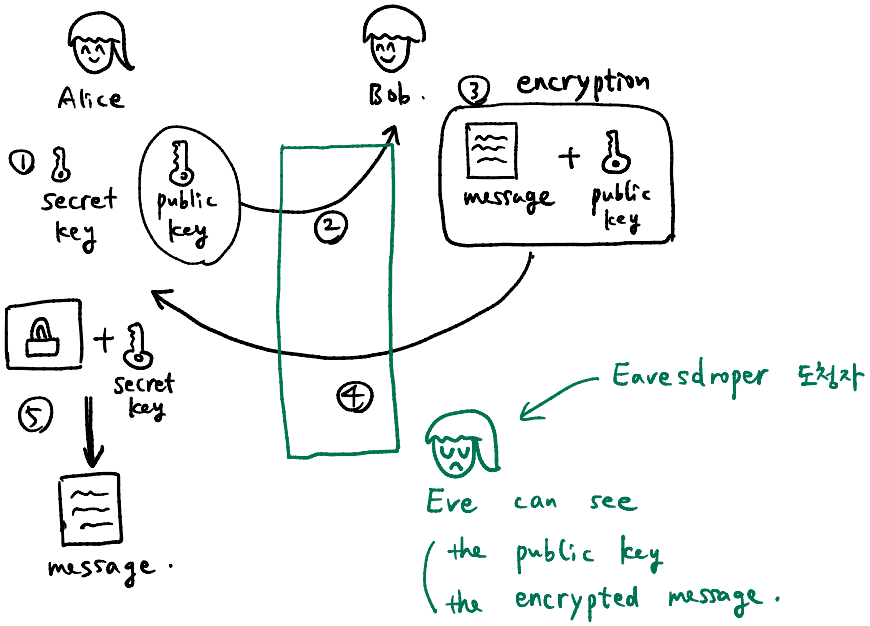
6-2 Quantum Cryptography (§12.6)

QKD (Quantum Key Distribution) – public key cryptography vs private key cryptography

public key cryptography



RSA cryptosystem (Appendix 5)

① select large prime numbers p, q (using primality test, e.g., Miller-Rabin test)

② $n = pq,\ \phi = (p-1)(q-1)$

③ select small odd integer e s.t. $\phi/e \neq$ integer

④ find integer d s.t. $ed = 1 \pmod{\phi}$ (using the extended Euclidean algorithm)

⑤ public key $P = (e, n)$, secret key $S = (d, n)$

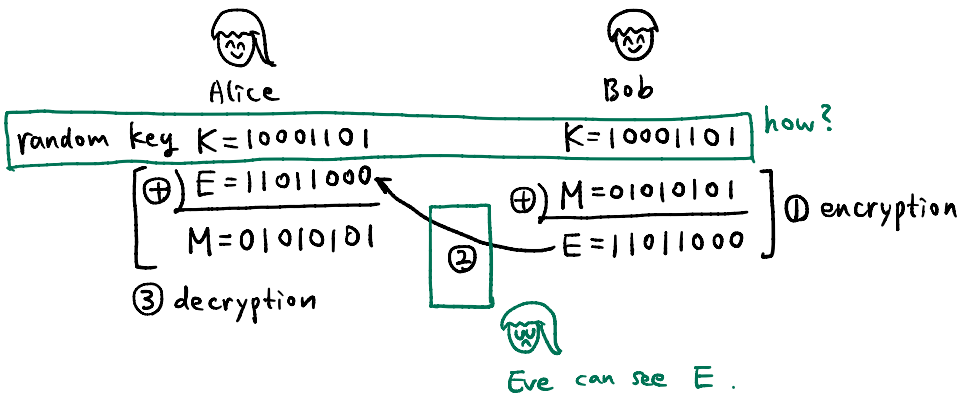
⑥ message $M < n$

⑦ encryption: $E(M) = M^e \pmod{n}$

⑧ decription: $D(E(M)) = E(M)^d \pmod{n} = M \pmod{n}$

💬 If Eve can find p, q from n (factoring), this cryptosystem is broken down!

private key cryptography



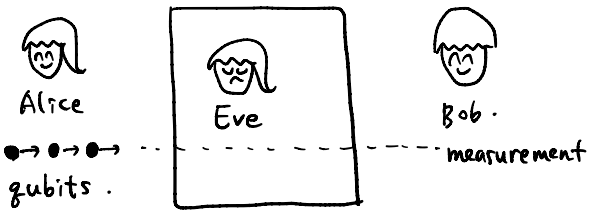
BB84 protocol

simplified version of Bennett & Brassard, 1984

You can distinguish between $|0\rangle$ and $|1\rangle$ (if you know the basis)

$|+\rangle$ and $|-\rangle$ (X-basis)

You can NOT distinguish between $|0\rangle$ and $|+\rangle$ (unless you have many copies)



Eve(eavesdropper) can do anything that quantum mechanics allows!

① Alice sends qubits to Bob. Each qubit is chosen randomly from $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$.

basis Z: $\{|0\rangle, |1\rangle\}$ basis X: $\{|+\rangle, |-\rangle\}$

$|0\rangle$, $|+\rangle$ mean 0 $|1\rangle$, $|-\rangle$ mean 1

Bob, Eve do not know the bases.

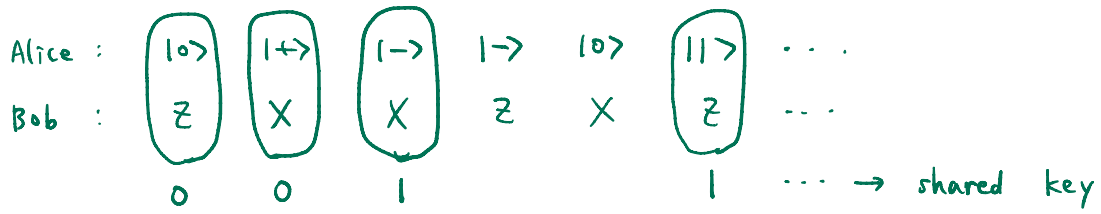
② Bob measures each qubit in randomly chosen basis Z or X.

③ Alice and Bob announce their bases.

④ They take qubits sent and measured in the same bases.

⑤ Half of the qubits in ④ are used to check eavesdropping.

The other half are the shared key bits.



What can Eve do?

HW6-3 Alice sends $|+\rangle$ $|1\rangle$ $|+\rangle$ $|+\rangle$ $|+\rangle$ $|1\rangle$ $|0\rangle$ $|0\rangle$ $|-\rangle$ $|+\rangle$

Bob measures X Z Z X X Z X X X Z

What is the key Alice and Bob obtain? (including the bits for the security check)