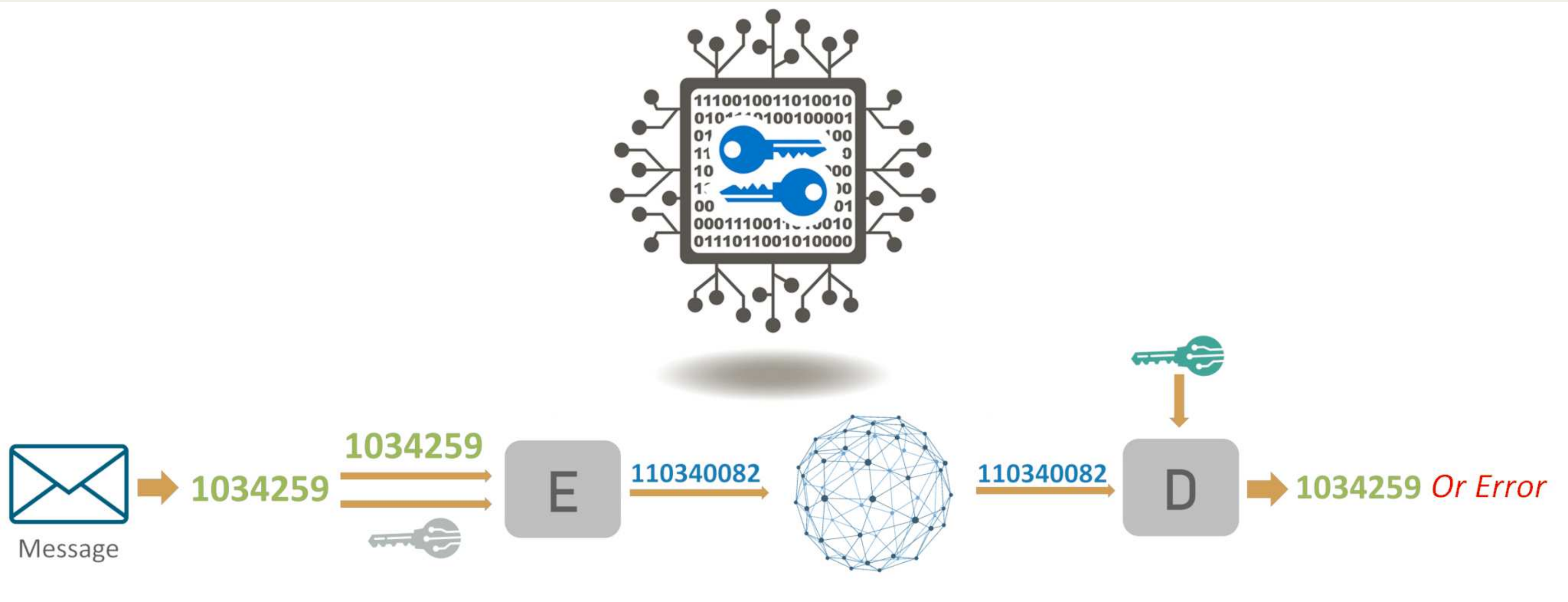
Amsterdam University of Applied Sciences

Quantum Key Distribution

Quantum Capita Selecta

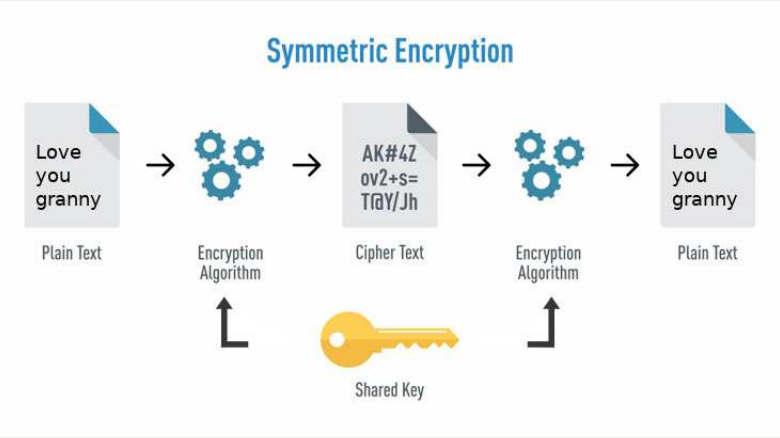
Bernardo Villalba Frías, PhD
b.r.villalba.frias@hva.nl

Cryptography



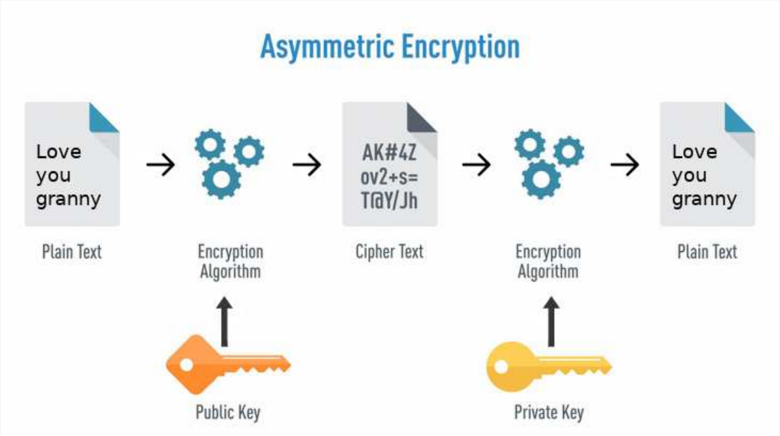
- “Secure communication and data in the presence of third parties”
- Caesar cipher (100–44 BC)
- Enigma (WWII)
- Today: RSA, AES

Symmetric–key encryption



- Same key for encryption and decryption
- Private key shared between two or more parties
- Examples:
  - AES, Twofish, Serpent
- Downside:
  - Secure channel for key exchange
  - Too many keys

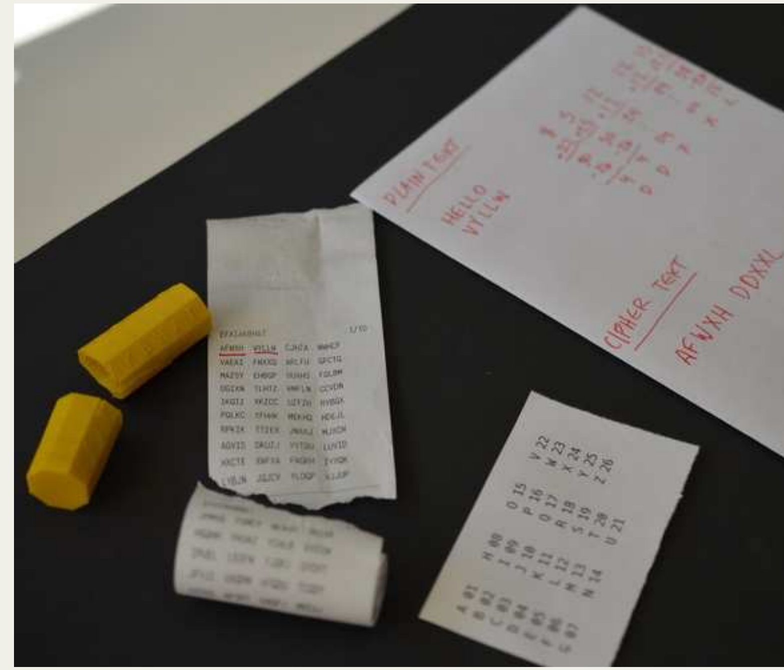
Asymmetric–key encryption



- Different key for encryption and decryption
  - Public key: widely disseminated
  - Private key: known only by the owner
- Examples:
  - RSA, Elliptic–curve cryptography
- Downside:
  - Widespread security compromise

One–time pad (OTP)

- Symmetric–key encryption
- Modular addition (XOR)
  - Message and key
- Impossible to break if the key is:
  1. Truly random
  2. Key length $\geq$ message length
  3. Never reused
  4. Secret



One–time pad (OTP)

Amsterdam University of Applied Sciences

Encoding

$$\text{Message} = 1\,1\,1\,1\,1\,0\,0\,0\,0\,0 \rightarrow m_i$$
$$\text{Key} = 0\,1\,0\,1\,1\,1\,0\,0\,1\,0 \rightarrow k_i$$
$$\text{Encoded message} = 1\,0\,1\,0\,0\,1\,0\,0\,1\,0 \rightarrow e_i = m_i \oplus k_i$$

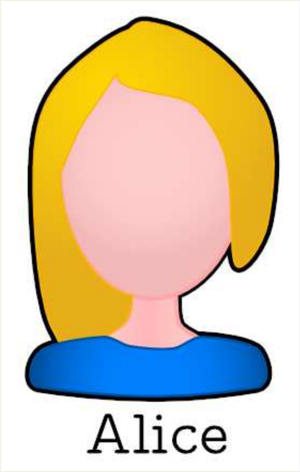
Decoding

$$\text{Encoded message} = 1\,0\,1\,0\,0\,1\,0\,0\,1\,0 \rightarrow e_i$$
$$\text{Key} = 0\,1\,0\,1\,1\,1\,0\,0\,1\,0 \rightarrow k_i$$
$$\text{Decoded message} = 1\,1\,1\,1\,1\,0\,0\,0\,0\,0 \rightarrow e_i \oplus k_i = m_i$$

$$e_i \oplus k_i = (m_i \oplus k_i) \oplus k_i = m_i \oplus (k_i \oplus k_i) = m_i \oplus 0 = m_i$$

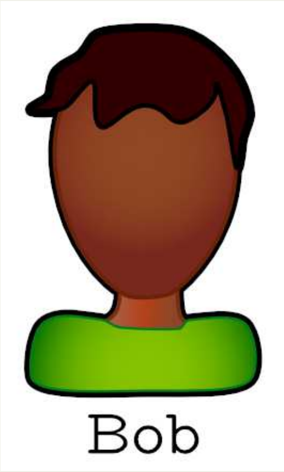
How to establish a secret key?

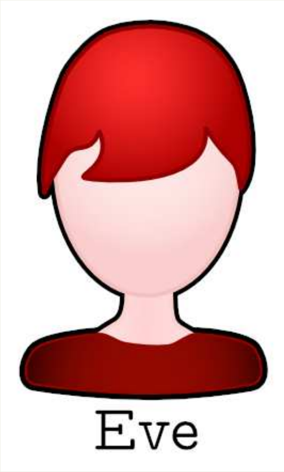
- We need a secure channel to share the secret key



1) Pre–share secret key

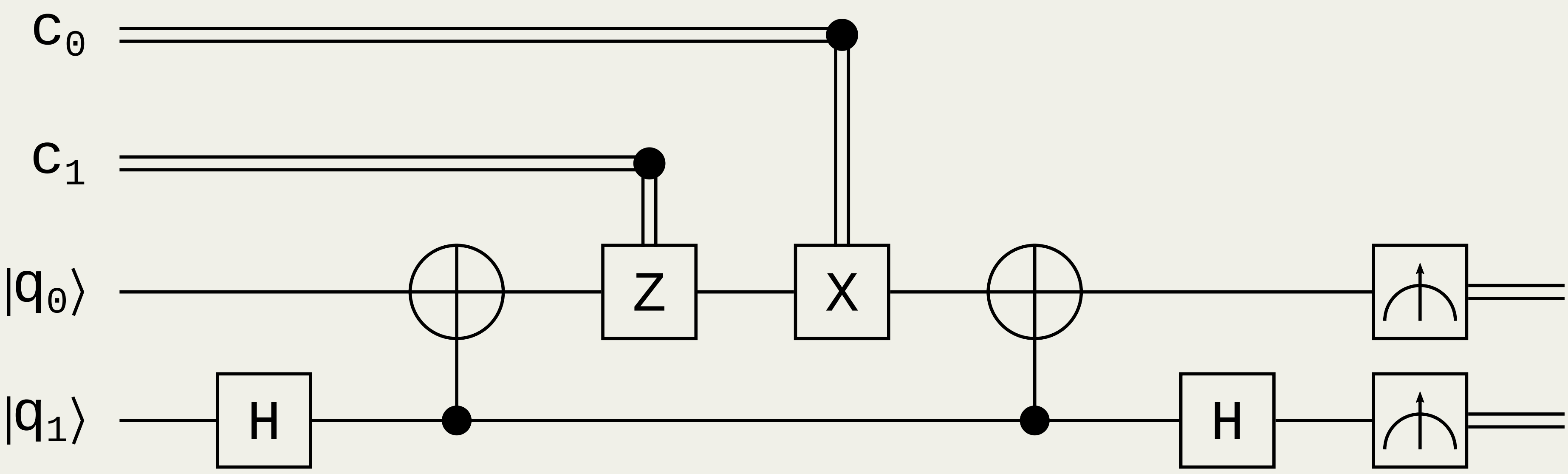
2) Encrypted messages





Superdense coding

- Transmit two bits by sending one qubit



Quantum Key Distribution

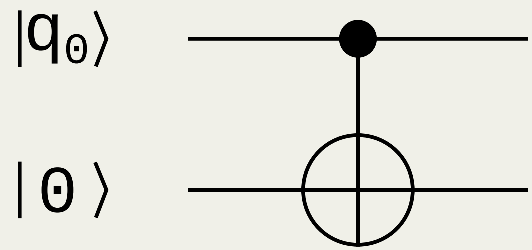
Amsterdam University of Applied Sciences

- A provably secure protocol
- Allows to create private keys bits between two parties over a public channel
- These keys can be used to implement a classical private–key cryptosystem
- Security of key is based on principles of quantum information
  - No–cloning theorem
  - Information gain implies disturbance

No–cloning theorem

Amsterdam University of Applied Sciences

- No quantum circuit can clone an arbitrary quantum state
- However, orthogonal states can be cloned



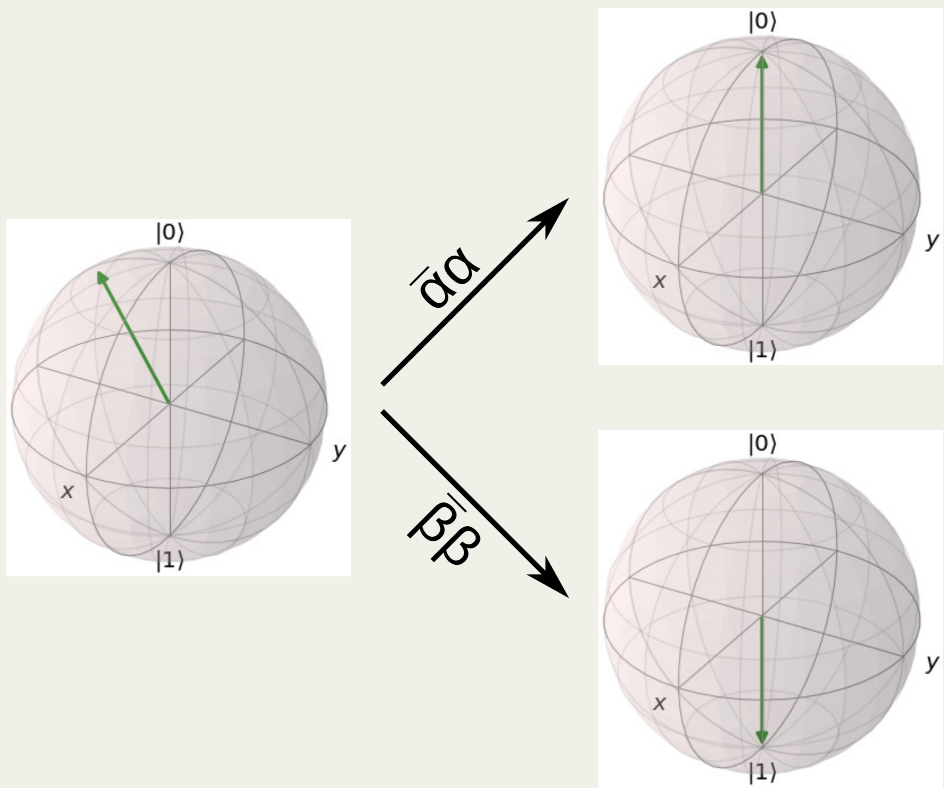
$$\begin{aligned} |q_0\rangle &= |0\rangle \\ &\rightarrow |0q_0\rangle \\ &\rightarrow |00\rangle \\ \mathit{CNOT}_{0,\,1} &\rightarrow |00\rangle \end{aligned}$$

$$\begin{aligned} |q_0\rangle &= |1\rangle \\ &\rightarrow |0q_0\rangle \\ &\rightarrow |01\rangle \\ \mathit{CNOT}_{0,\,1} &\rightarrow |11\rangle \end{aligned}$$

$$\begin{aligned} |q_0\rangle &= |+\rangle \\ &\rightarrow |0q_0\rangle \\ &\rightarrow |0+\rangle \\ &\rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) \\ \mathit{CNOT}_{0,\,1} &\rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \end{aligned}$$

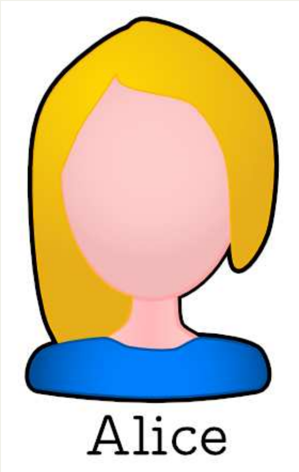
Information gain implies disturbance

- Measurements are destructive
- Any attempt to distinguish between two non–orthogonal quantum states disturbs the signal

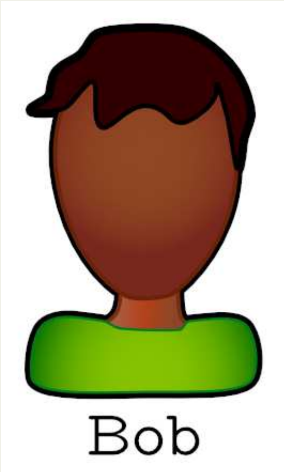


BB84 protocol

- Eight step protocol which requires Alice and Bob to:



  - Have true random number generators
  - Share a classical authenticated channel
  - Share a quantum channel
  - Prepare and measure in the computational (Z) and X basis



BB84 protocol

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

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

- Alice sends the resulting qubit $|q_i\rangle$ to Bob

Alice:	B_i	X	Z	X	Z	Z	X	X	X	Z	X	X	X
	b_i	0	1	1	0	0	0	1	0	1	0	1	0
	q_i	$\lvert +\rangle$	$\lvert 1\rangle$	$\lvert -\rangle$	$\lvert 0\rangle$	$\lvert 0\rangle$	$\lvert +\rangle$	$\lvert -\rangle$	$\lvert +\rangle$	$\lvert 1\rangle$	$\lvert +\rangle$	$\lvert -\rangle$	$\lvert +\rangle$

BB84 protocol

Amsterdam University of Applied Sciences

- Bob measures 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
- Alice and Bob repeat the previous steps a large number of times (N)

	B_i	X	Z	X	Z	Z	X	X	X	Z	X	X	X
Alice:	b_i	0	1	1	0	0	0	1	0	1	0	1	0
	q_i	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$
	B_i	Z	Z	X	X	Z	X	Z	X	X	Z	Z	X
Bob:	m_i	1	1	1	0	0	0	0	0	1	1	1	0
	q_i	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$

BB84 protocol

- Alice and Bob publicly announce the N bases they have each used. Importantly, Alice does not reveal her b_i nor does Bob reveal his m_i
- Alice and Bob sift out the $M \leq N$ runs in which they used the same basis ($B_i = \widetilde{B_i}$) and throw away the rest.

	B_i	X	Z	X	Z	Z	X	X	X	Z	X	X	X
Alice:	b_i	0	1	1	0	0	0	1	0	1	0	1	0
	q_i	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$
	B_i	Z	Z	X	X	Z	X	Z	X	X	Z	Z	X
Bob:	m_i	1	1	1	0	0	0	0	0	1	1	1	0
	q_i	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$

BB84 protocol

- Alice and Bob randomly pick a subset of the sifted pairs (b_i, m_i) and compare them using a classical communication channel. If the outcomes correlate perfectly, they can confidently use the remaining ones as a sifted key!

	B_i	Z	X	Z	X	X	X
Alice:	b_i	1	1	0	0	0	0
	q_i	$\lvert 1\rangle$	$\lvert -\rangle$	$\lvert 0\rangle$	$\lvert +\rangle$	$\lvert +\rangle$	$\lvert +\rangle$
	B_i	Z	X	Z	X	X	X
Bob:	m_i	1	1	0	0	0	0
	q_i	$\lvert 1\rangle$	$\lvert -\rangle$	$\lvert 0\rangle$	$\lvert +\rangle$	$\lvert +\rangle$	$\lvert +\rangle$

Sifted key: 1 0 0 0

BB84 protocol

Amsterdam University of Applied Sciences

- Randomness in selecting the basis B_i and $\widetilde{B_i}$ ensures a 75% of correctness in the message

$$\{B_i,\, b_i\} \to \begin{cases} B_i = \widetilde{B_i} & 50\% \\ B_i \neq \widetilde{B_i} & \begin{cases} b_i = m_i & 25\% \Rightarrow 75\% \\ b_i \neq m_i & 0\% \end{cases} \end{cases}$$

- Eavesdroppers have to randomly pick a basis $\overline{B_i}$, hence disturbance is introduced

BB84 protocol

- To detect an eavesdropper with probability 99.9999% $\rightarrow$ need to compare 72 bits
- As a post–processing step, Alice and Bob apply additional operations on the remaining bits to obtain a shared private key:
  - Information reconciliation (e.g. cascade protocol)
  - Privacy amplification (e.g. hash function)

BB84 protocol

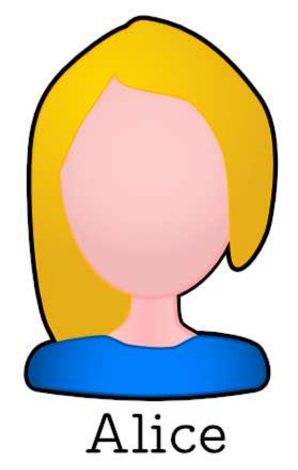
- Limited quantum complexity
  - Preparation to zero state, Pauli X gate, Hadamard gate, and measurement in the computational basis.
- Secure
  - Key is truly random (generated by Alice)
  - Eavesdroppers can be detected
- Large overhead

BB84 protocol

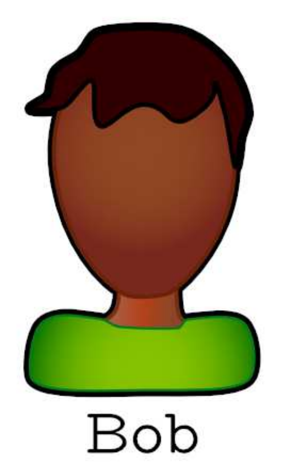
- QKD is already commercially available!

E91 protocol

- Based on Bell states (generated by any source)
- Uses 3 measurement basis:
  - Alice: $\left\{Z_0,\, Z_{\frac{\pi}{8}},\, Z_{\frac{\pi}{4}}\right\}$
  - Bob: $\left\{Z_0,\, Z_{\frac{\pi}{8}},\, Z_{-\frac{\pi}{8}}\right\}$
- Same requirements as BB84



- Have true random number generators
- Share a classical authenticated channel
- Share Bell states



E91 protocol

Amsterdam University of Applied Sciences

- The entangled qubits are distributed between Alice and Bob and they:
  - Randomly choose a measurement basis
  - Measure their qubits and store the results
  - Announce their measurement basis
  - Two groups of qubits are created:
    - Group A: measured with the same basis
      - Used to generate the key
    - Group B: measured with different basis
      - Used to detect eavesdroppers (correlation measurement)

E91 protocol

- More quantum complexity compared to BB84
  - Preparation to zero state, Hadamard gate, CNOT gate, and measurement in the computational basis
  - Entangled states are sensitive to noise
- Secure
  - The key is undetermined until measurement (key generation)
  - Eavesdroppers can be detected

Other QKD protocols

- BB92 protocol
  - Based on BB84
  - Uses only 1 measurement basis
- Six–States protocol
  - Similar to BB84 with an additional basis
- Coherent One Way protocol
  - Tailored for weak coherent qubits
- Differential Phase Shift protocol
  - Randomized phase modulation of the qubits


Questions?