Introduction to Quantum Computing

Week 6: Quantum Encryption in Action

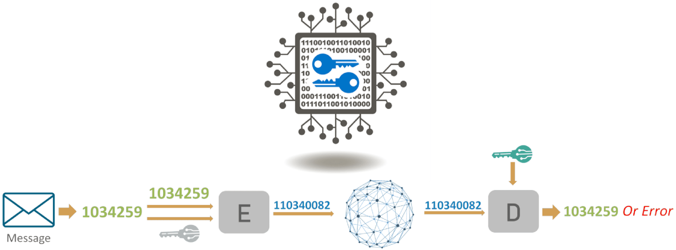
Bernardo Villalba Frías, PhD

b.r.villalba.frias@hva.nl

Quantum Talent and Learning Center
Amsterdam University of Applied Sciences

Week 6
13th June 2025

Cryptography



- "Secure communication and data in the presence of third parties"
- Symmetric–key encryption
- Asymmetric–key encryption

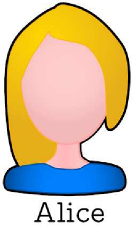
Quantum Key Distribution

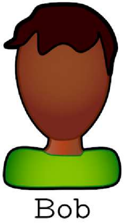
- Key exchange protocol between two remote users via:
  - An *insecure* quantum channel:
    - An adversary can perform arbitrary quantum operations on transmitted quantum systems
  - An *authenticated* classical channel:
    - Messages can be read by the adversary but not modified
- Proven to be *information-theoretically secure* (under certain assumptions)
- The exchanged 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

The BB84 Protocol

Requirements

- Assuming that the quantum theory is correct...
- Eight step protocol which requires Alice and Bob to:
  - Operate within secured locations using only trusted devices and adhering strictly to the protocol
  - Have true random number generators
  - Share a classical authenticated channel
  - Share a quantum channel
  - Prepare and measure in the computational (Z) and X basis





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	$\lvert+\rangle$	$\lvert 1\rangle$	$\lvert-\rangle$	$\lvert 0\rangle$	$\lvert 0\rangle$	$\lvert+\rangle$	$\lvert-\rangle$	$\lvert+\rangle$	$\lvert 1\rangle$	$\lvert+\rangle$	$\lvert-\rangle$	$\lvert+\rangle$

Protocol

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

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$_i$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$

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

Sifted key: 1 0 0 0

Performance

- Randomness in selecting the basis B_i and $\widetilde{B}_i$ would ensure a 75% of correctness in the message

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

- However, when $B_i \neq \widetilde{B}_i$, it is just "chance"
- $\Rightarrow$ better be safe
- Eavesdroppers have to randomly pick a basis $\overline{B_i}$, hence disturbance is introduced

Post–processing

- 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)

Characteristics

- 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

Thank you

Thank you!