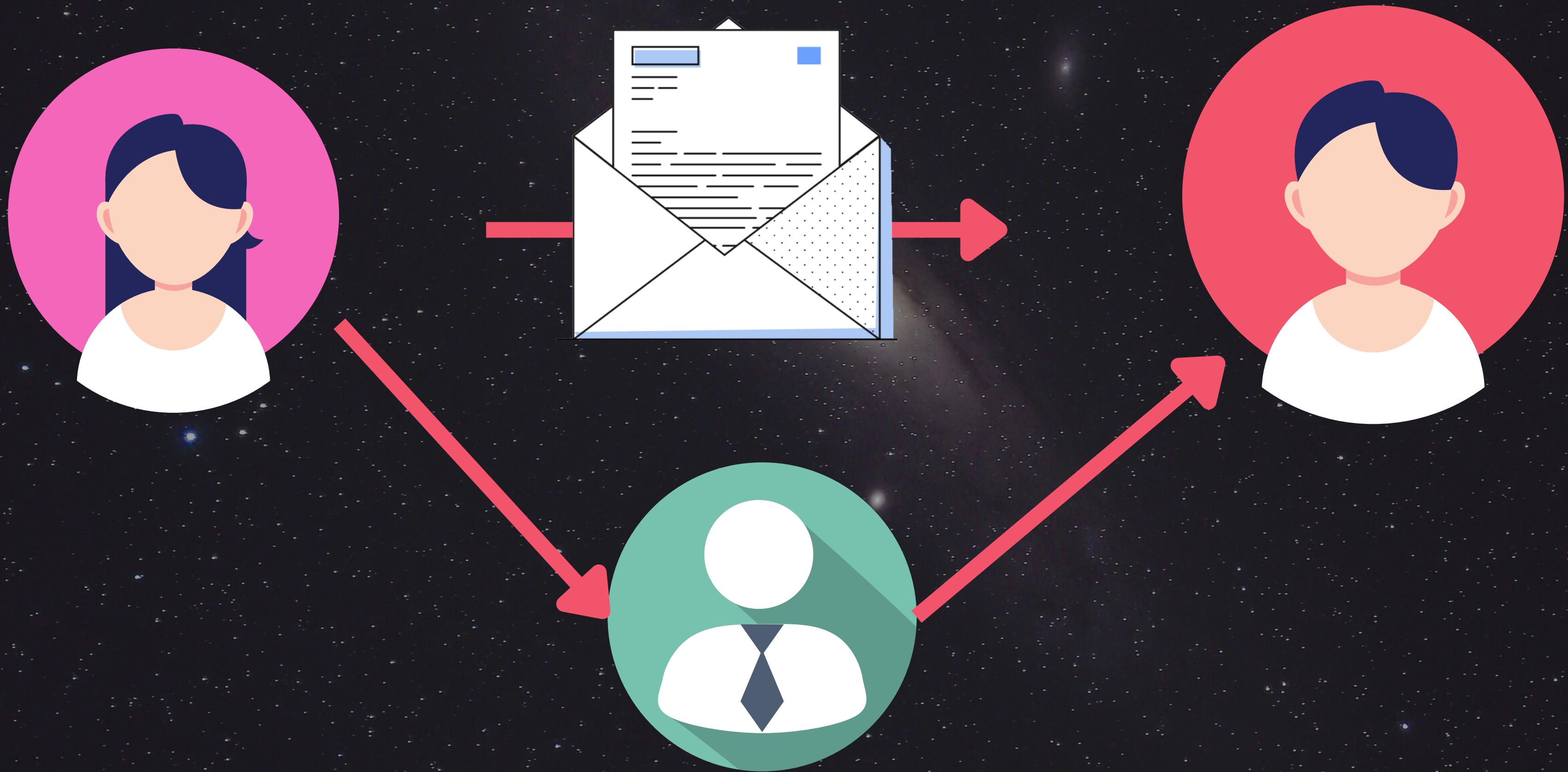




# Estudio del Modelo de Encriptación BB84

Kevin Dannie Guzmán Duran - 2211875

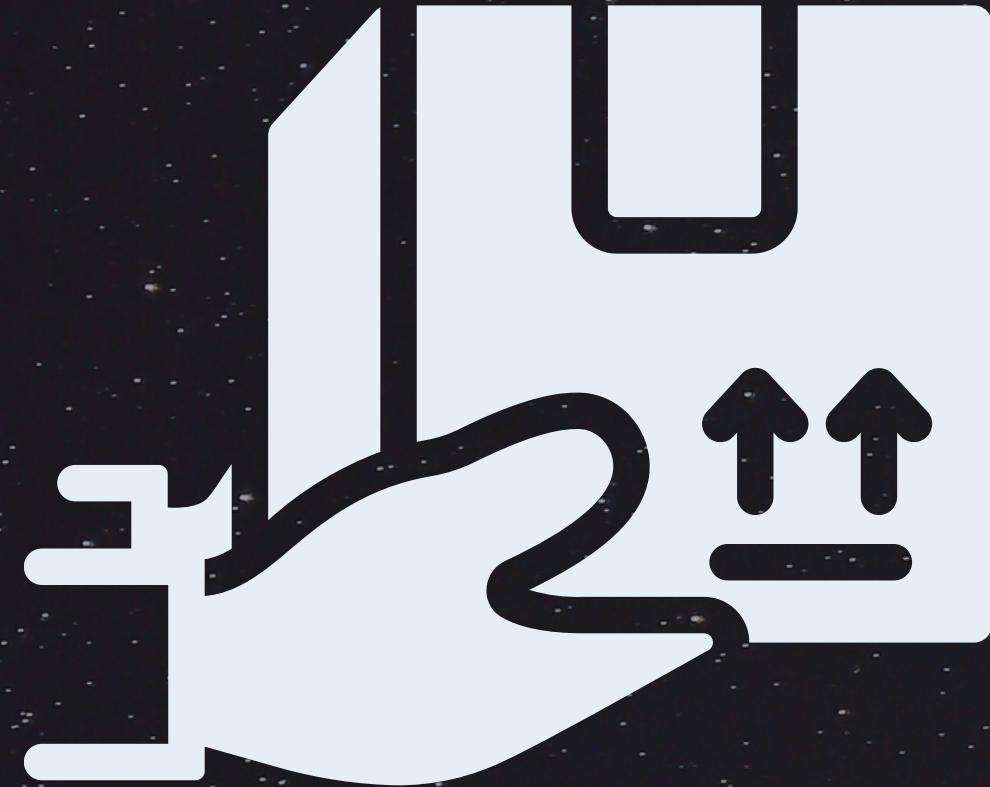
# UN POCO DE CONTEXTO



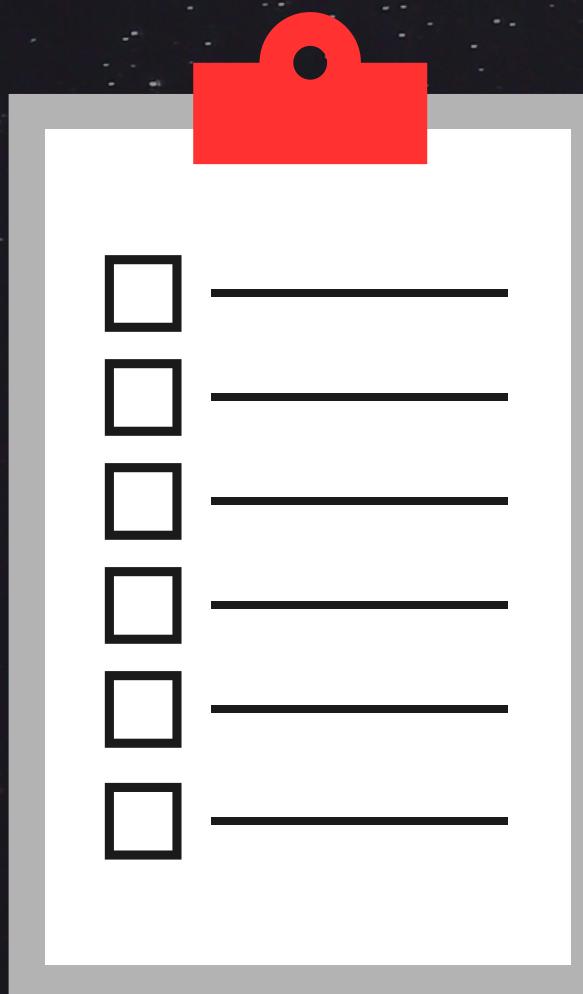
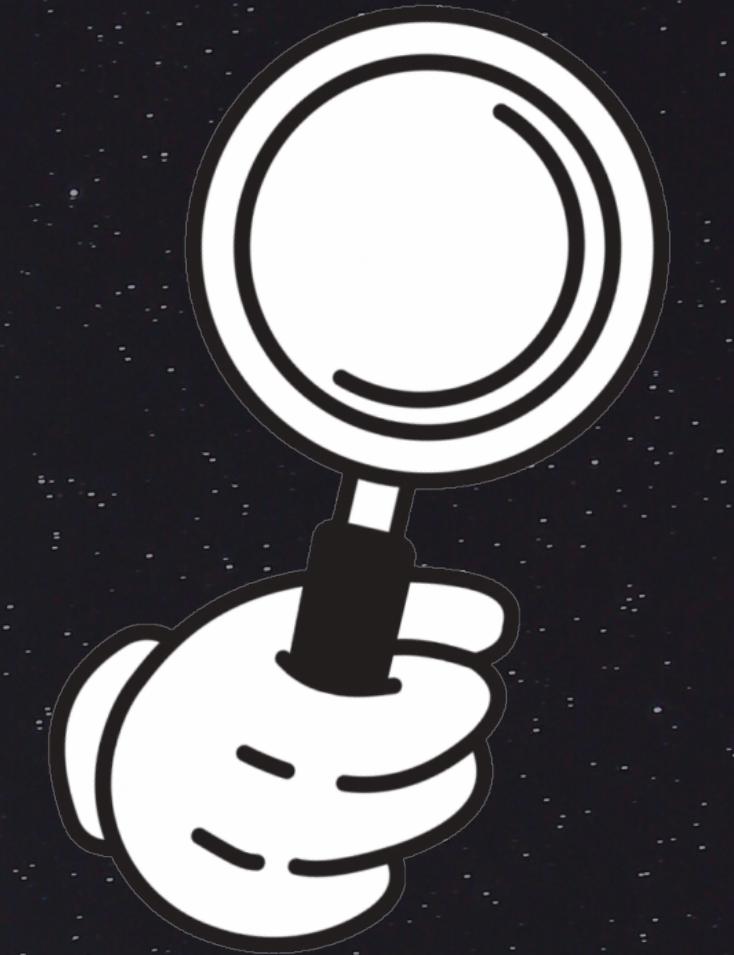
## Bases de los qubits

## El valor de los qubits

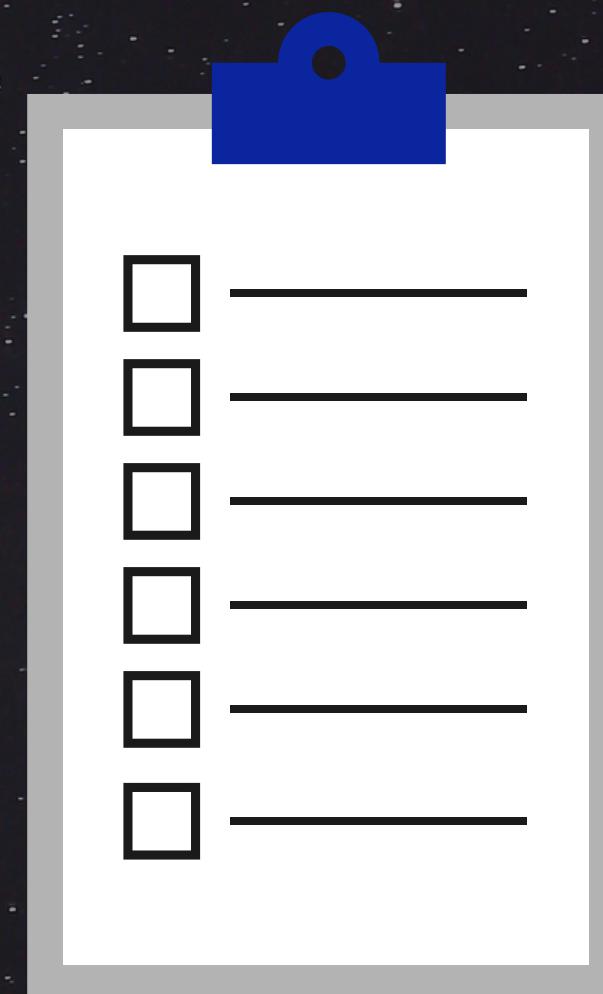




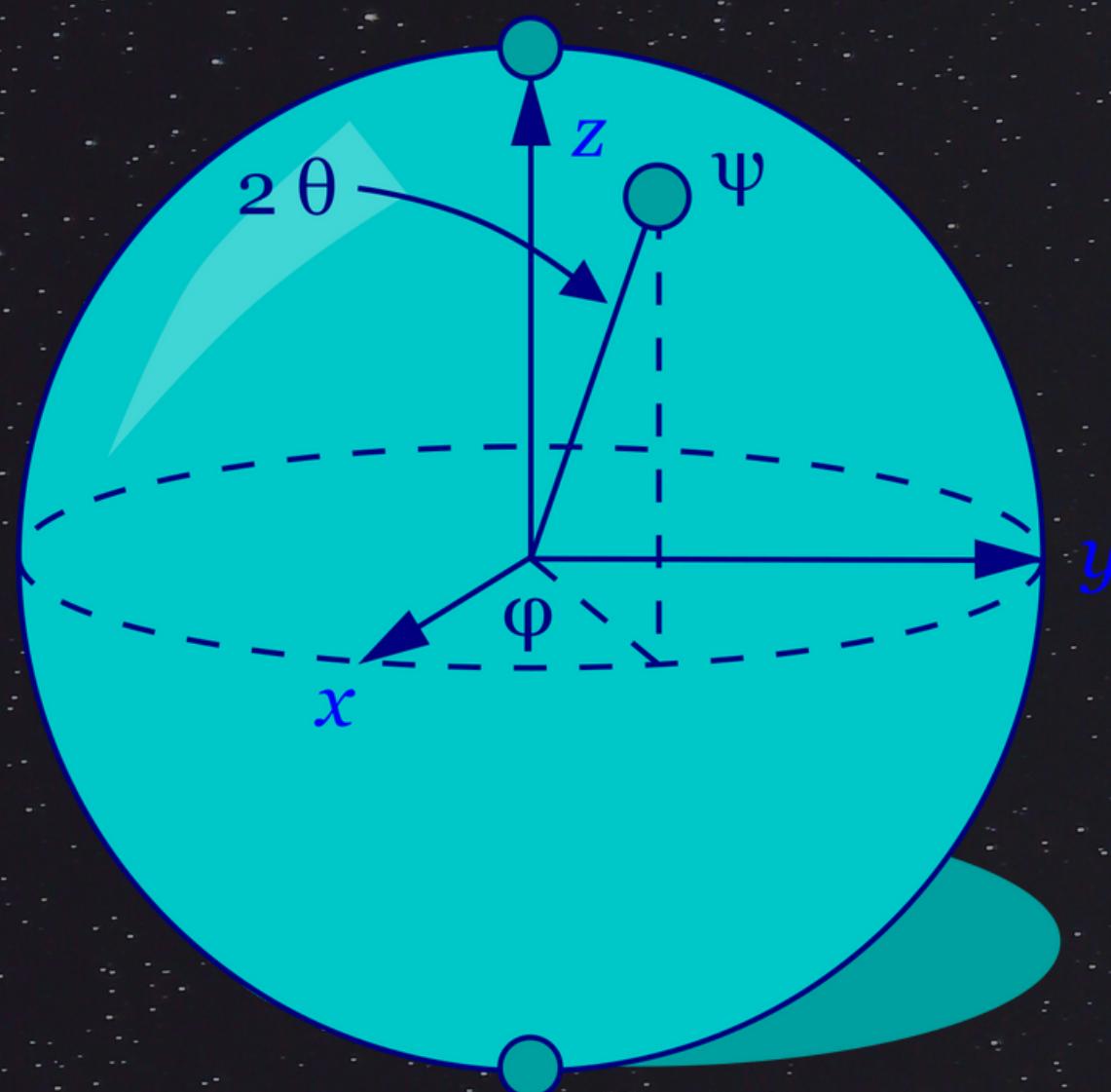
Bob evalúa sin  
conocer las bases de  
Alice



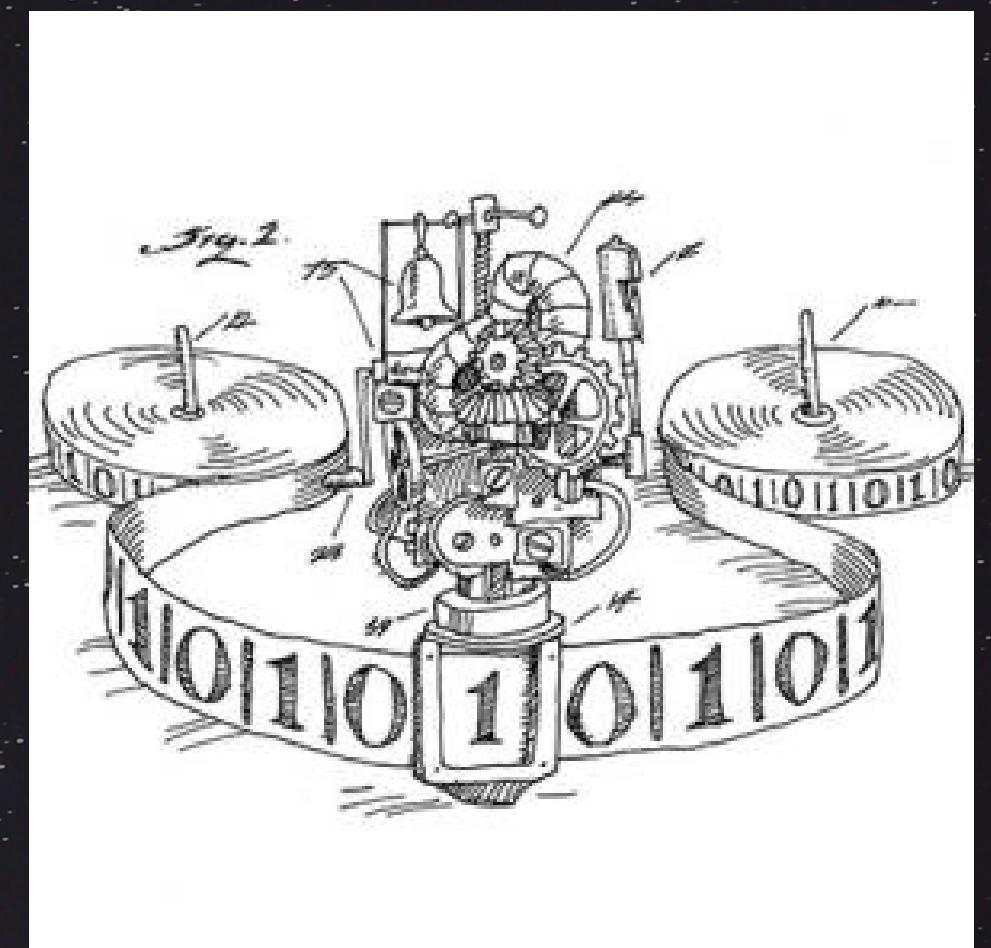
Finalmente ambos  
tienen una libreta  
con los qubits



# CONCEPTOS A UTILIZAR



Para crear los qubits se hará uso de un AFD y para encriptar las palabras se hará uso de la Maquina de Turing.

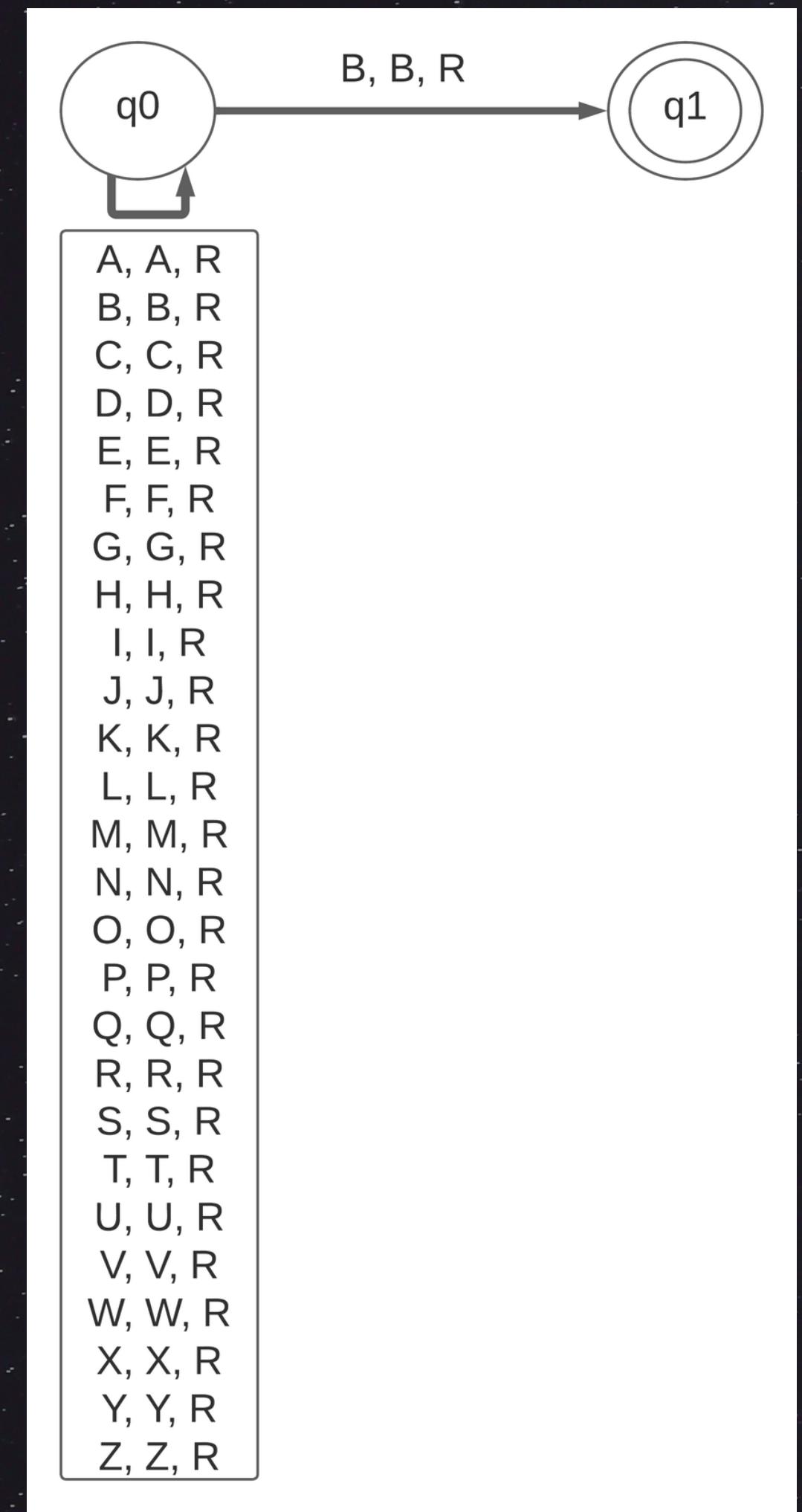


# ESTADO DEL ARTE

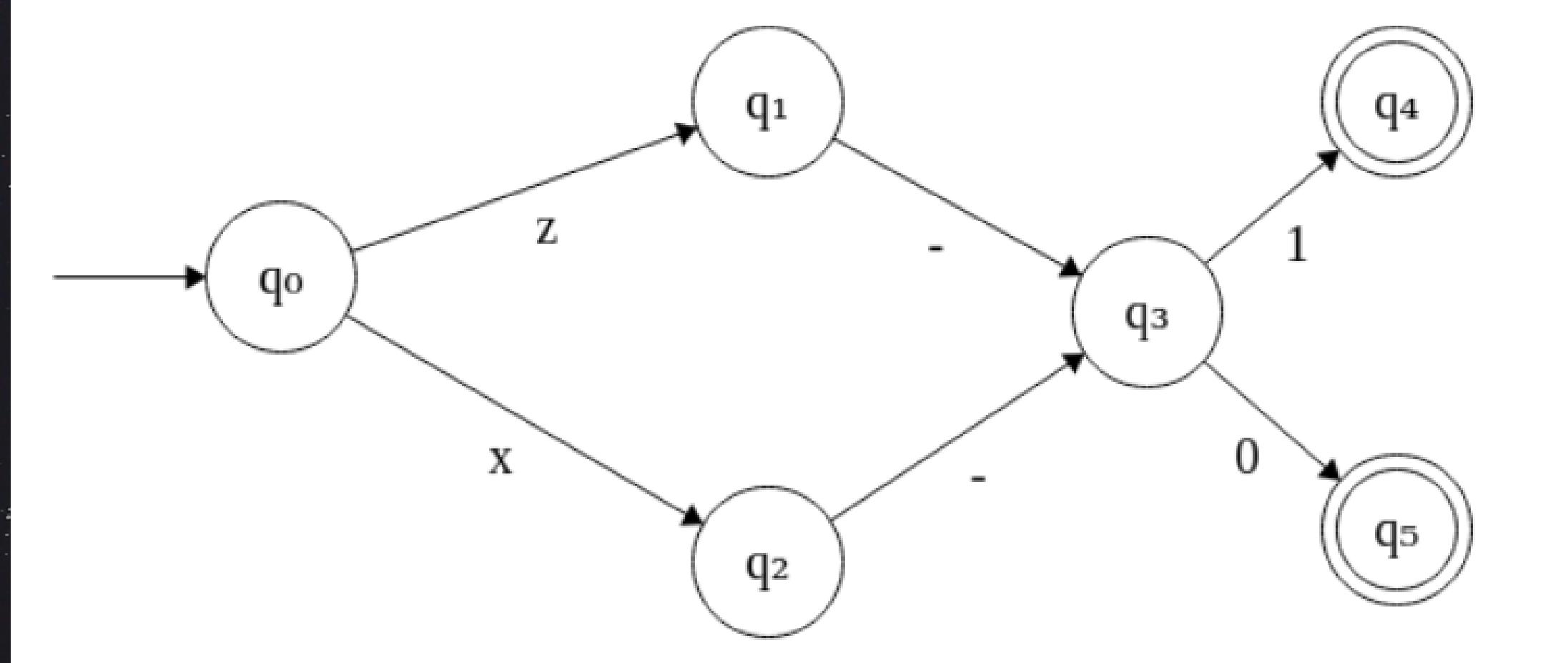
Encriptado de texto  
Mediante el método Cesar

Sebastian Contreras





# Diagrama de la maquina de Turing y del Automata Finito Determinista



# Definición Formal de la Maquina de Turing

$M\Gamma = (Q, q_0, F, \Sigma, \Gamma_B, \delta)$   $Q = \{q_1, q_2\}$  Estado inicial:  $q_0$

$\Sigma = \{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S,$

$T, U, V, W, Y, Z, ', ''\}$

$F = \{q_1\}$   $B = ''$

$\Gamma = \{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q,$

$R, S, T, U, V, W, Y, Z, '', '''\}$

# Definición Formal del Autómata Finito Determinista

$$A = (Q, \Sigma, \delta, q_0, F) \quad Q = \{q_0, q_1, q_2, q_3, q_4, q_5\}$$

$$F = \{q_4, q_5\} \quad \Sigma = \{'z', 'x', '^', '1', '0'\} \quad \text{Estado inicial: } q_0$$

$$q_0, \delta(q_0, 'z') = q_1 \quad q_0, \delta(q_0, 'x') = q_2 \quad q_1, \delta(q_1, '^') = q_3$$

$$q_2, \delta(q_2, '^') = q_3 \quad q_3, \delta(q_3, '0') = q_5 \quad q_3, \delta(q_3, '1') = q_4$$

# RESULTADOS

Por medio del AFD y la maquina de Turing se logró encriptar la palabra deseada, por medio del método de encriptacion BB84

```
['Z', 'Y', 'X', 'W', 'V', 'U', 'T', 'W', 'R', 'Q', 'P', 'O', 'N', 'S', 'L', 'K', 'J', 'I', 'H', 'G', 'F', 'E', 'D', 'C', 'B', 'A']
MESSI
TMConfiguration('q1', TMCTape('SEWWJ..', 6))
```

**¡GRACIAS POR SU  
ATENCIÓN!**