Quantum Cryptography: BB84

Moh Kashani

Agenda

01 What is cryptography?

02 What is key distribution?

03 What is quantum key distribution?

04 What is BB84?

05 What is post-quantum cryptography?

06 Conclusion

What is cryptography?

Transmit

Active Eavesdropper

Passive Eavesdropper

Cryptography: Encoding data using mathematics and algorithms.

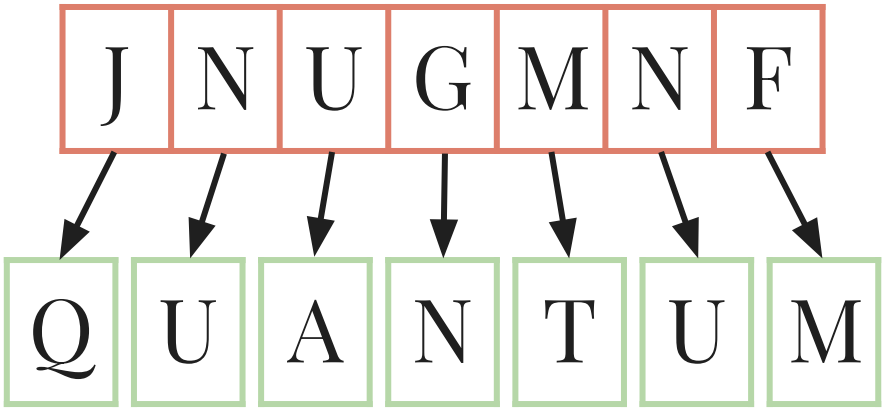
How cryptography was used?

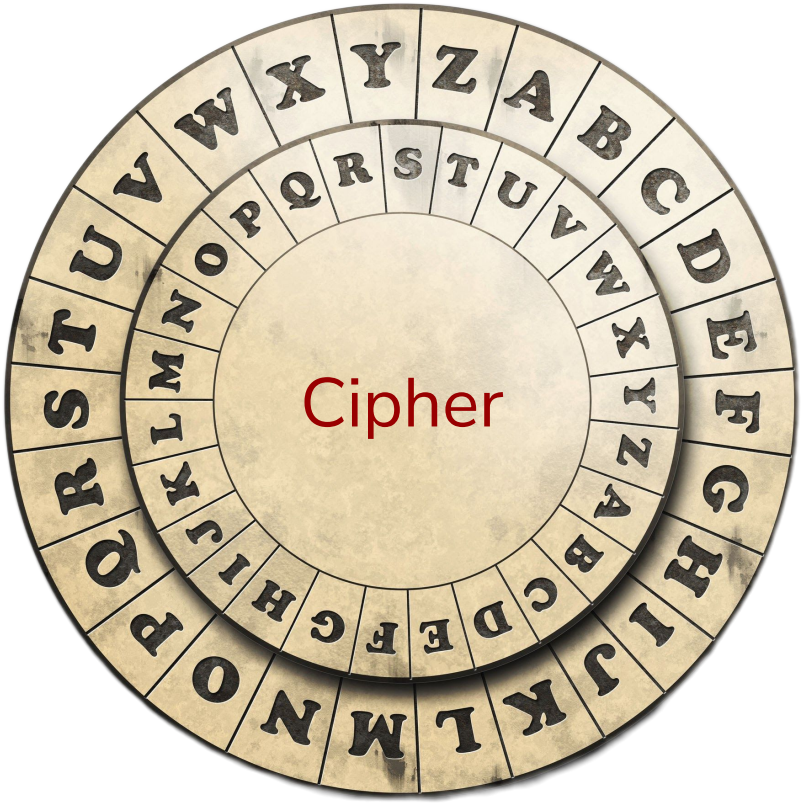
Encrypt

Transmit

Decrypt

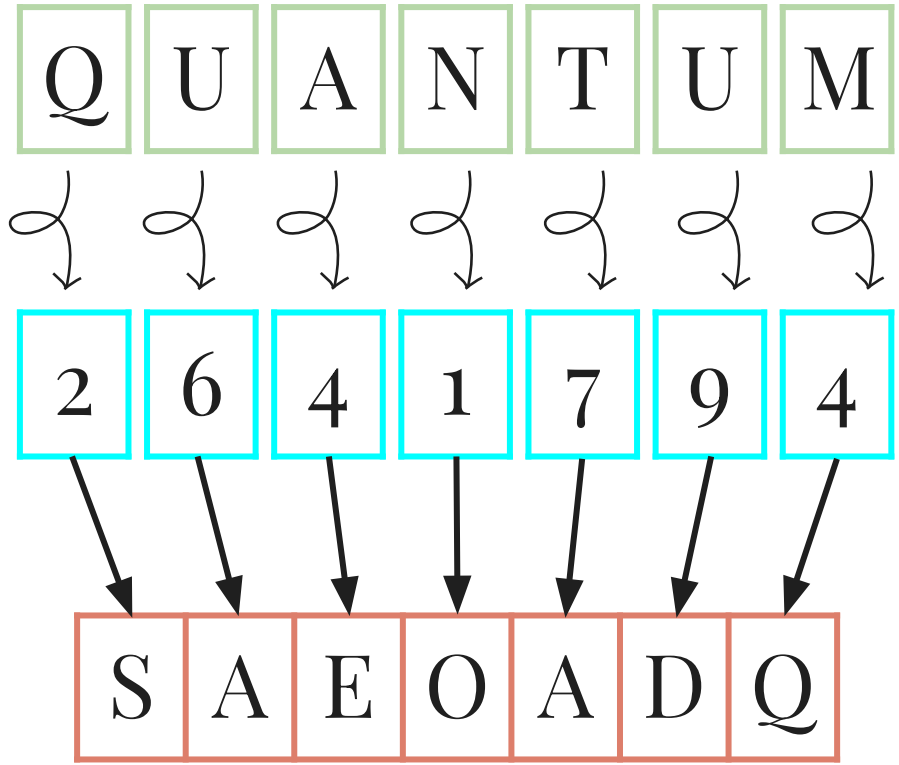
Caesar Cipher





Better secrecy

Random shift per letter

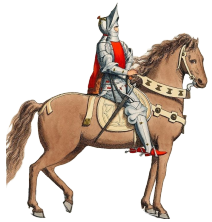


Question?

How does the general know the letter shift?

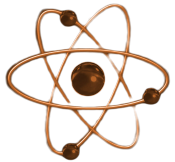
Quantum Key Distribution (QKD)?

E	O	A	D	Q



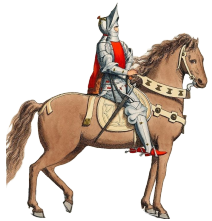
Classical Channel

6	4	1	7	9

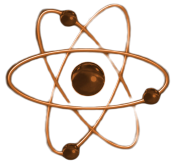


Quantum Channel

Why Quantum Channel is safe?



- Vulnerable to Eavesdropping



- No-cloning theorem
  - Eavesdropping active or passive is detectable

What is BB84?

Bennett

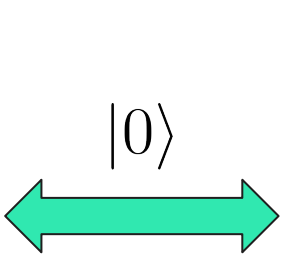
Brassard

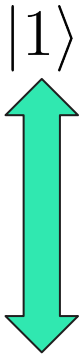
How does the quantum channel work?

Classical Channel

Quantum Channel

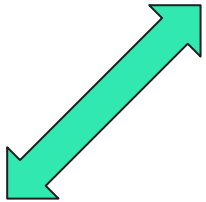
Light Polarization

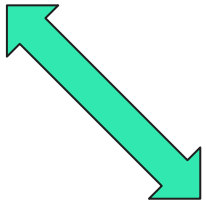




Rectilinear Polarization

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

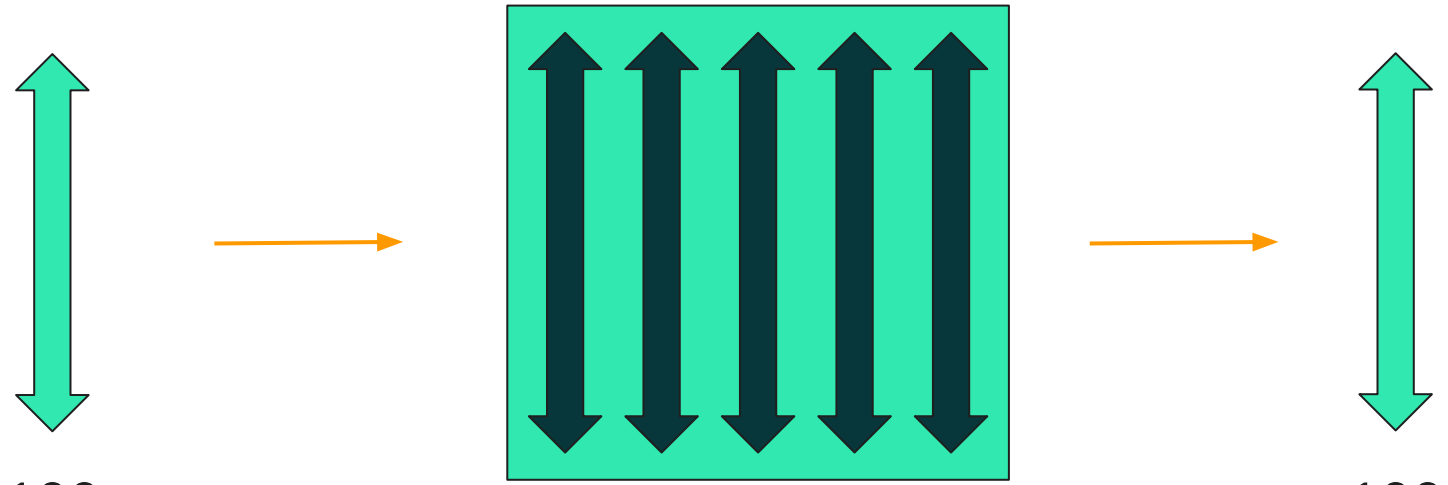




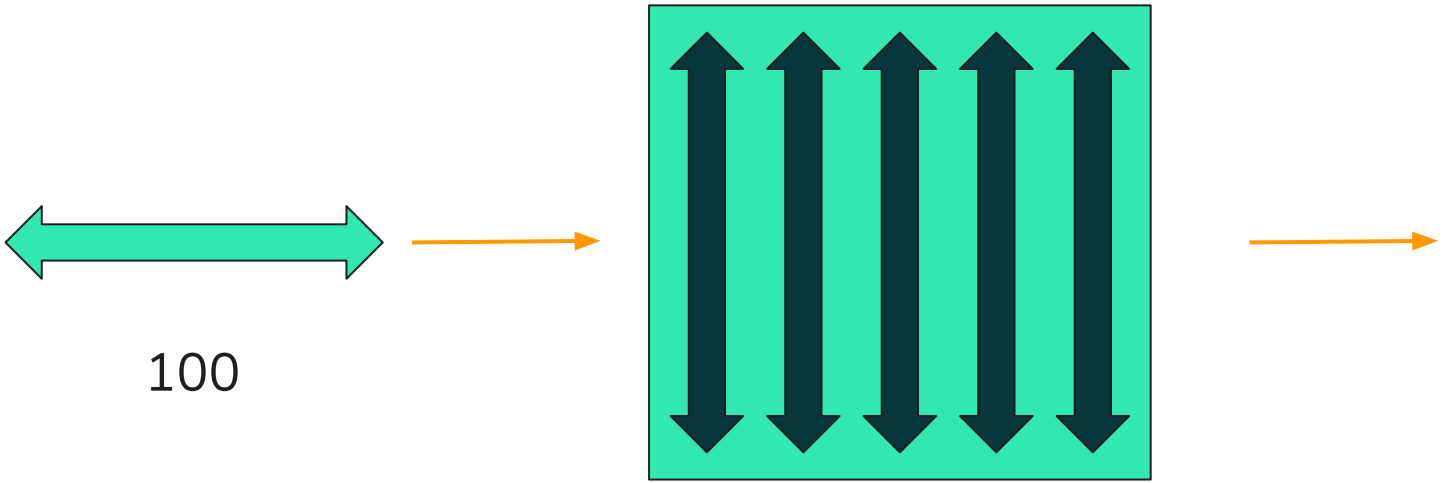
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Diagonal Polarization

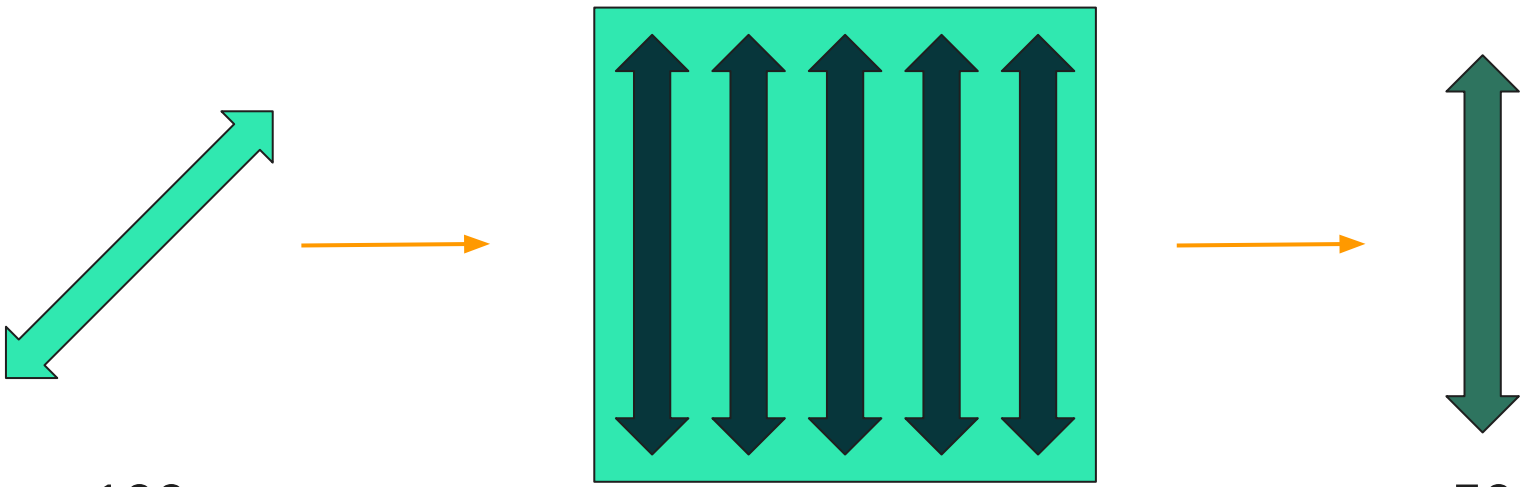
Light Polarization



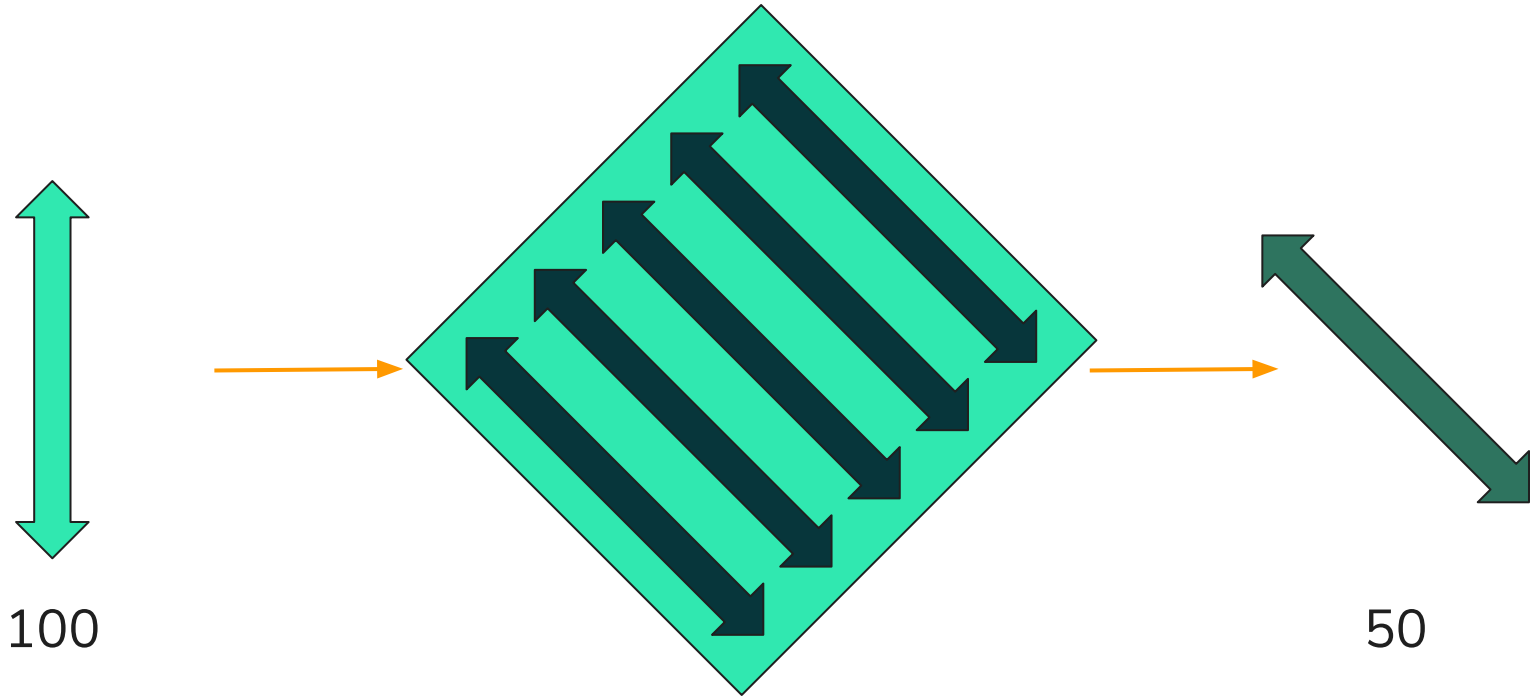
Light Polarization



Light Polarization



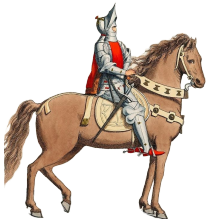
Light Polarization



Light polarization in action

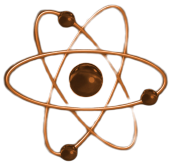
Quantum Key Distribution (QKD)?

E O A D Q



Classical Channel

6 4 1 7 9



Quantum Channel

What is BB84?

1. Alice choose random bits
2. Alice choose random bases (light polarization) for each bit

   |

   Transmitting

   |
3. Bob randomly chooses a base (polizer) to measure the data

Alice's random bits	0	1	1	0	1	1	0	0
Random sending bases	D	R	D	R	R	R	R	R
Photons Alice sends	⤢	↕	⤡	↔	↕	↕	↔	↔
Random receiving bases	R	D	D	R	R	D	D	R
Bits as received by Bob	1		1		1	0	0	0

? ?

What is BB84?

1. Bob reveals ⅓ of the basis it has used for measurements
2. Alice confirms the bases that align with its chosen base

3. From those good bases Bob randomly transmits received bits
   a. This make sure that there was no eavesdropper

QUANTUM TRANSMISSION								
Alice's random bits	0	1	1	0	1	1	0	0
Random sending bases	D	R	D	R	R	R	R	R
Photons Alice sends	⤢	↕	↘	↔	↕	↕	↔	↔
Random receiving bases	R	D	D	R	R	D	D	R
Bits as received by Bob	1		1		1	0	0	0
PUBLIC DISCUSSION								
Bob reports bases of received bits	R		D		R	D	D	R
Alice says which bases were correct			OK		OK			OK
Presumably shared information (if no eavesdrop)			1		1			0
Bob reveals some key bits at random					1			
Alice confirms them					OK			
OUTCOME								
Remaining shared secret bits			1					0

What is BB84?

QUANTUM TRANSMISSION								
Alice's random bits	0	1	1	0	1	1	0	0
Random sending bases	D	R	D	R	R	R	R	R
Photons Alice sends	⤢	↕	↘	↔	↕	↕	↔	↔
Random receiving bases	R	D	D	R	R	D	D	R
Bits as received by Bob	1		1		1	0	0	0
PUBLIC DISCUSSION								
Bob reports bases of received bits	R		D		R	D	D	R
Alice says which bases were correct			OK		OK			OK
Presumably shared information (if no eavesdrop)			1		1			0
Bob reveals some key bits at random					1			
Alice confirms them					OK			
OUTCOME								
Remaining shared secret bits			1					0

Post-Quantum Cryptography

Classic **Quantum** **Post-Quantum**

Thank you!