Ananya Teklu

Creating Secure Encryptions with Quantum Cryptography

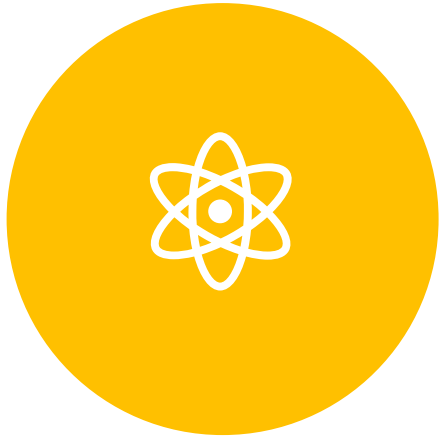
Why do we need encryptions?

ENCRYPTION HELPS

SEND SENSITIVE INFORMATION OVER THE INTERNET

STORE OUR DATA ON THE CLOUD SECURELY

CURRENT ENCRYPTION SYSTEMS USE KEYS TO SCRAMBLE AND UNSCRAMBLE DATA. KEYS ARE GENERATED USING MATHEMATICAL PROBLEMS AND LOGIC.



IN THIS TALK I WILL BE TALKING ABOUT HOW WE CAN USE QUANTUM MECHANICS TO GENERATE KEYS TO ENCRYPT DATA

Outline

- Introduction ✓
- Background
- Quantum cryptography
  - Quantum key distribution
    - Prepare and measure protocols
    - Entanglement based protocols
- Implementation
- Conclusion

Background

Cryptography

- Is a science of hiding message with ''secret writing''
- Evidence shows its been in use since 2000 B.C
- The two modern cryptographic methods currently used are
    - Asymmetric cryptography (public key cryptography) uses pairs of keys public and private to encrypt and decrypt messages
        - RSA relies on the practical difficulty of factoring the product of two large prime numbers
    - Symmetric cryptography uses one key to encrypt and decrypt messages
        - One-Time-Pad

Background

Encoding Alphabets into binary

A	01000001	N	01001110
B	01000010	O	01001111
C	01000011	P	01010000
D	01000100	Q	01010001
E	01000101	R	01010010
F	01000110	S	01010011
G	01000111	T	01010100
H	01001000	U	01010101
I	01001001	V	01010110
J	01001010	W	01010111
K	01001011	X	01011000
L	01001100	Y	01011001
M	01001101	Z	01011010

Encoding the word FOOD

10000110 1001111 1001111 1000011

Background

Bitwise Exclusive Or (XOR)

- Represented with the symbol $\oplus$

A	B	A $\oplus$ B
0	0	0
0	1	1
1	0	1
1	1	0

Background

Making a simple encryption method

Encrypt “HELLO THERE’’

Key 00010001 00010001

Character	Binary
H	01001000
E	01000101
L	01001100
L	01001100
O	01001111
T	01010100
H	01001000
E	01000101
R	01010010

Encryption

”HELLO THERE”

Message 01001000 01000101 01001100 01001100 01001111 01010100 01001000 01000101 01010010 01000101

⊕

Key 00010001 00010001 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

Ciphertext 01011001 01010100 01001100 01001100 01001111 01010100 01001000 01000101 01010010 01000101

Decryption

Ciphertext 01001000 01000101 01001100 01001100 01001111 01010100 01001000 01000101 01010010 01000101

⊕

Key 00010001 00010001 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

Message 01011001 01010100 01001100 01001100 01001111 01010100 01001000 01000101 01010010 01000101

Frequency analysis attacks can be used on the

Background

One-Time-Pad (OTP)

Symmetric encryption technique that is unbreakable

Conditions for OTP to be unbreakable

Key must be truly random

Key at the minimum must be as long as the message

Key must never be reused in whole or in part

Key must be kept completely secret

Background

- One-Time-Pad (OTP)
  - Encoding the message into 0s and 1s
  - Generate random key
  - Bit wise XOR (⊕) of the key and encoded message

Binary Table

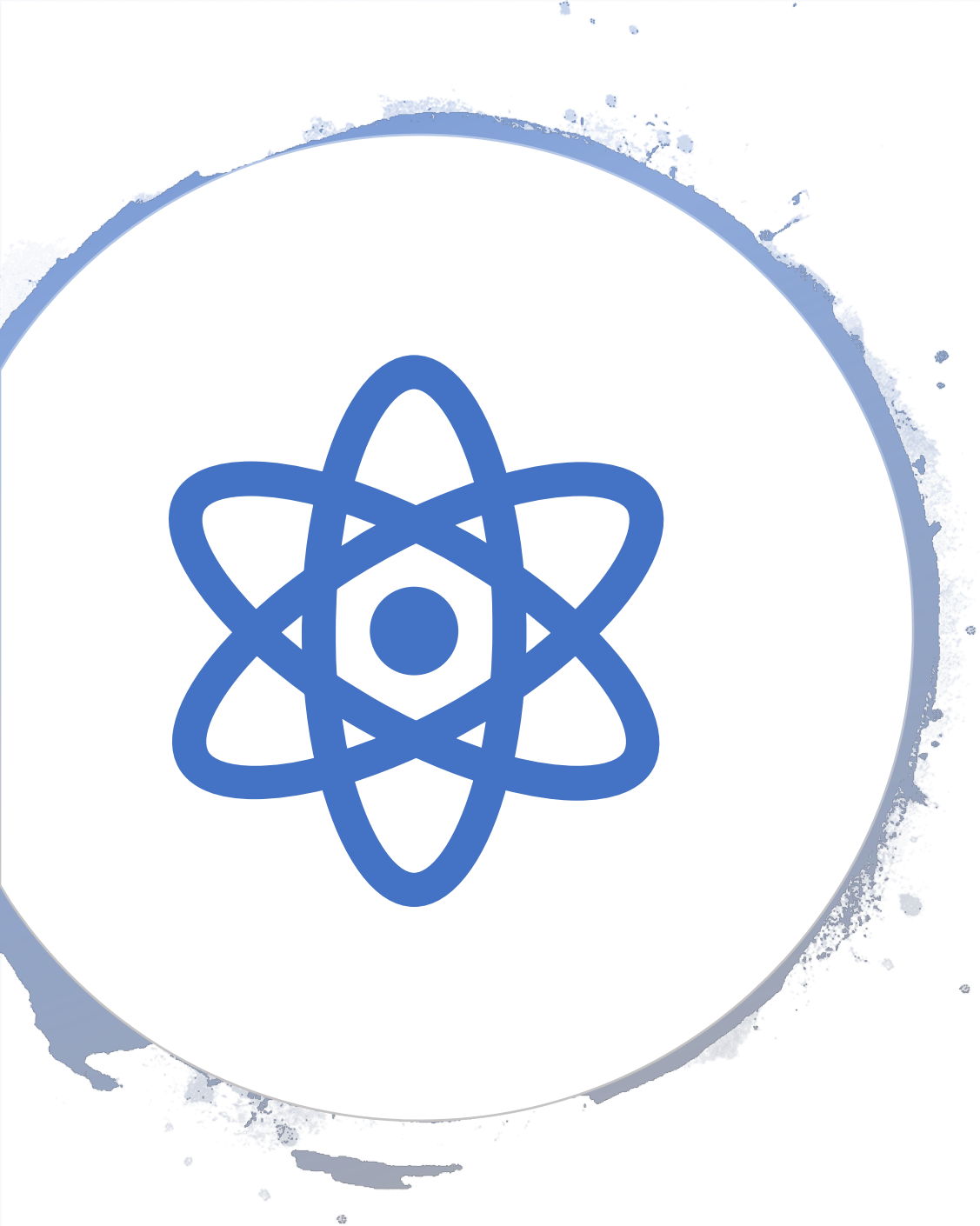
Character	Binary
H	01001000
E	01000101
L	01001100
L	01001100
O	01001111

Encrypting binary HELLO

Message	01001000 01000101 01001100 01001100 01001111
	⊕
Key	11100101 01000111 01110000 01010100 10101011
Ciphertext	10101101 00000010 00111100 00011000 11101100

Decrypting the ciphertext

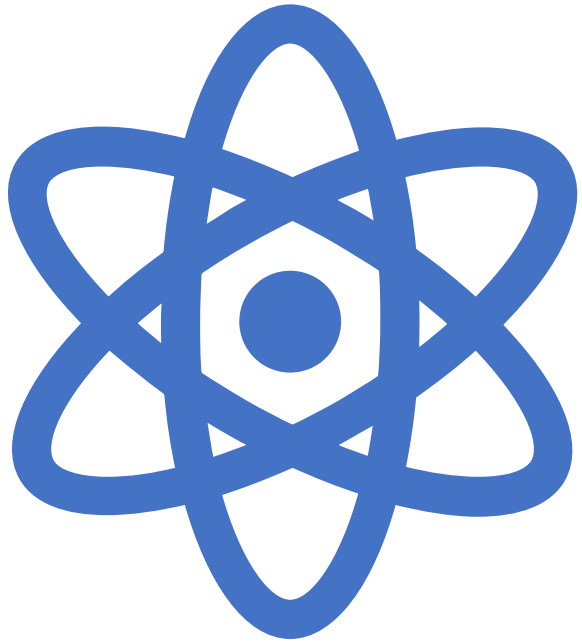
Ciphertext	10101101 00000010 00111100 00011000 11101100
	⊕
Key	11100101 01000111 01110000 01010100 10101011
Message	01001000 01000101 01001100 01001100 01001111



Background

Quantum Mechanics

- Heisenberg’s uncertainty principle
- Polarization of light and measurement
- No cloning theorem
- Entanglement



Background

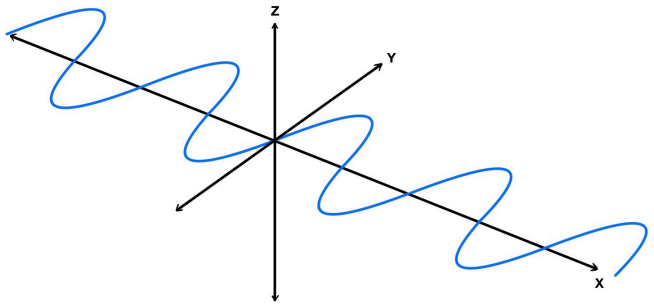
Heisenberg’s Uncertainty Principle

- Its impossible to know certain pairs of particles properties simultaneously
- Polarization of a photon is conjugate property

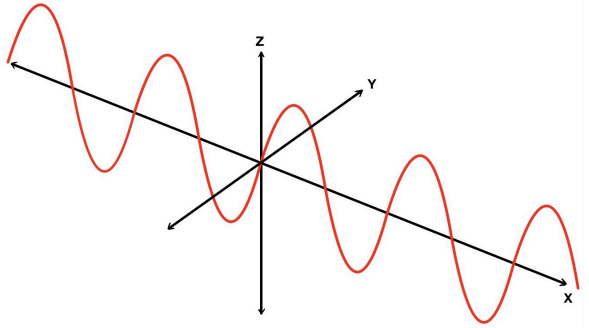
Background

Photons can be polarized in different directions

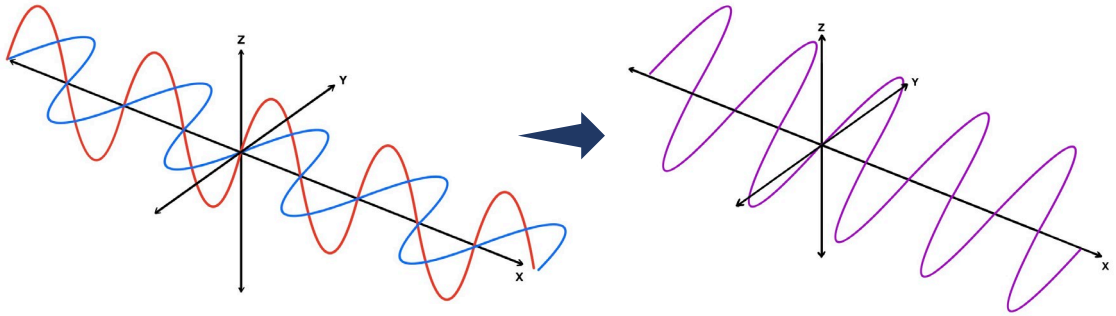
- Photons can be represented with electromagnetic waves



Horizontally (0°) polarized photon

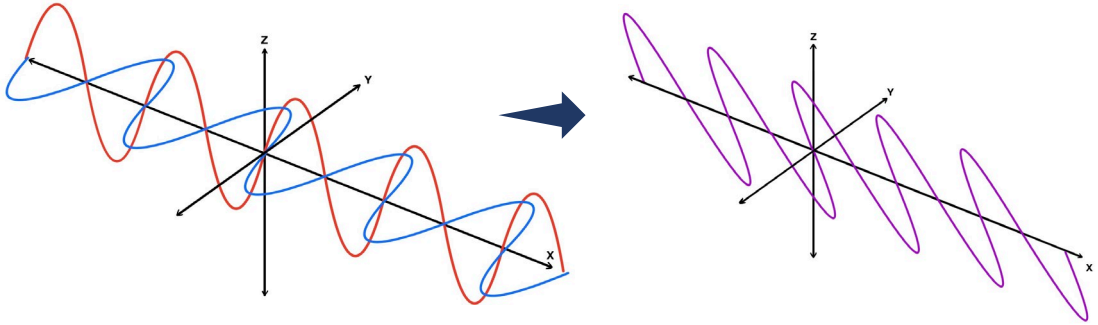


Vertically (90°) polarized photon



Superpositions of the horizontally and vertically polarized photon

45° polarized photon



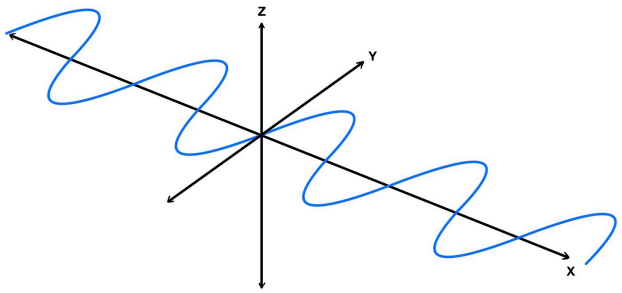
Superpositions of the horizontally and vertically polarized photon

135° polarized photon

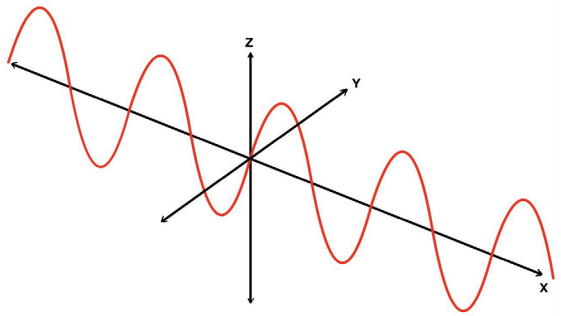
Background

Measurement of photons

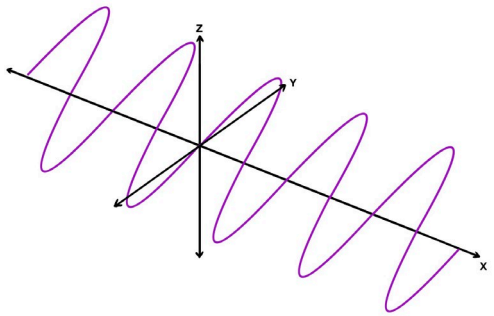
- Photons can be measured with polarizing filter



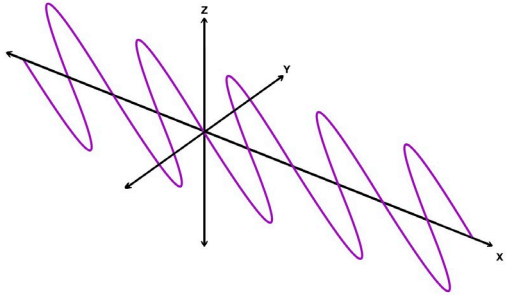
Horizontally (0°) polarized photon



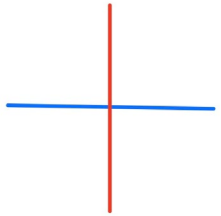
Vertically (90°) polarized photon



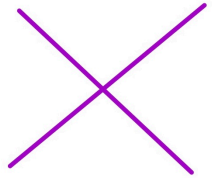
45° polarized photon



135° polarized photon



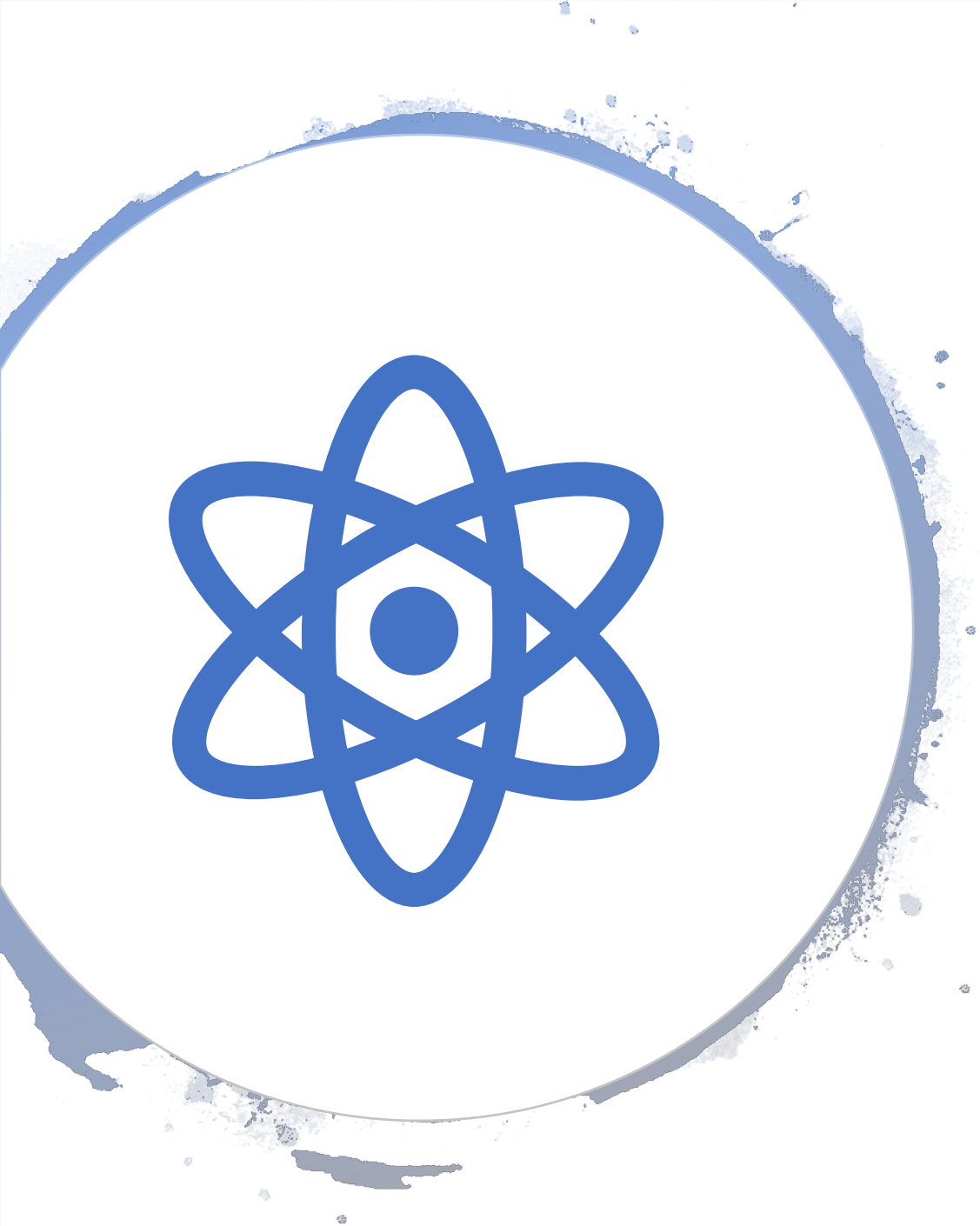
Rectilinear filter (basis)



Diagonal filter (basis)

Rectilinear measurement of (0°) and (90°) polarization encoded
(0°) equals bit 0 (90°) equals bit 1

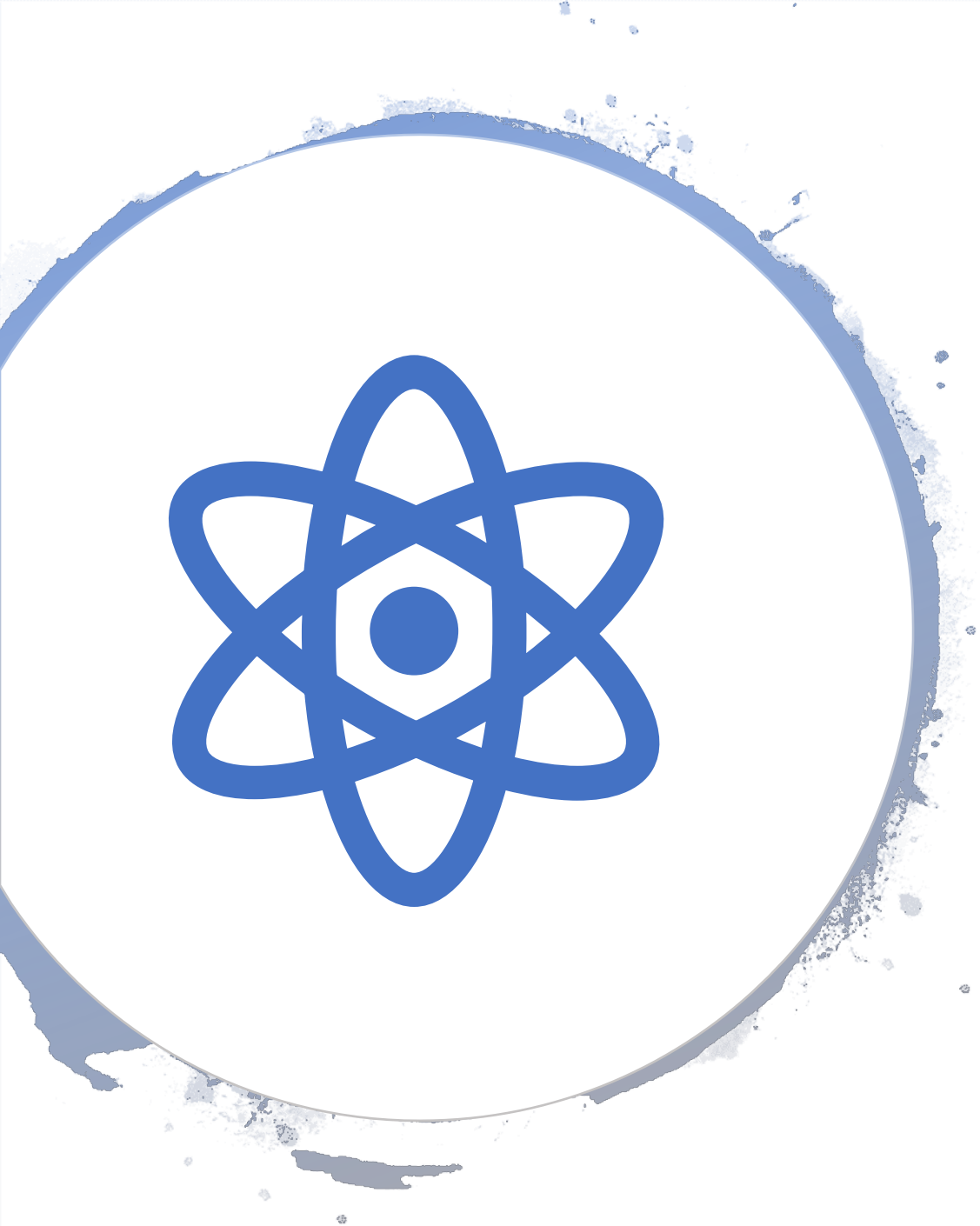
Diagonal measurement of (45°) and (135°) polarization encoded
(45°) equals bit 1 (135°) equals bit 0



Background

No Cloning theorem

- Its impossible to copy a quantum state
- Measurement is required to copy a quantum state



Background

Entanglement

- This is quantum phenomenon where two particles can exist in an entangled state
- A measurement on one of the particle's state will simultaneously change the other to be in an opposite state

Outline

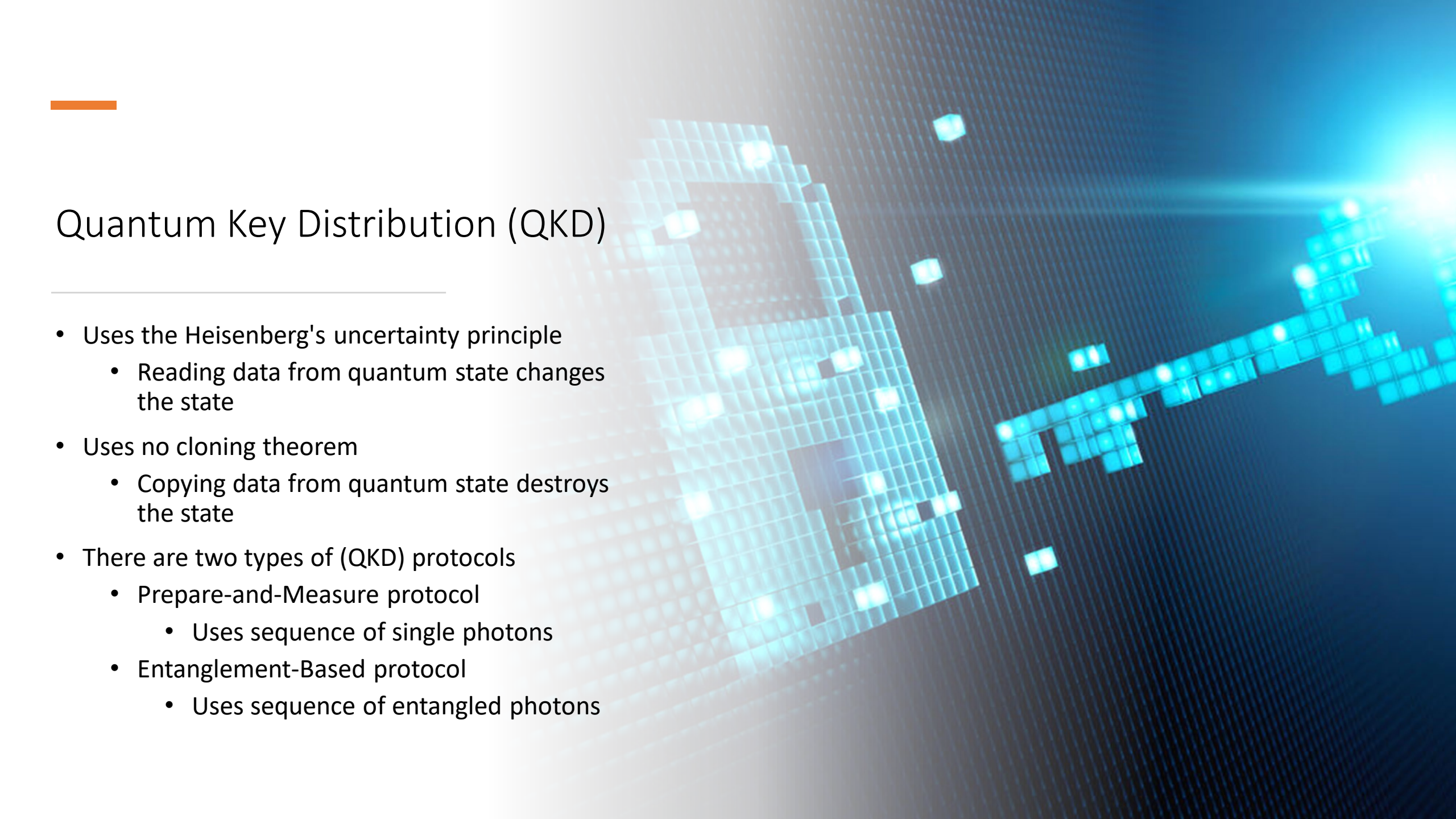
- Introduction ✓
- Background ✓
- Quantum cryptography
  - Quantum key distribution
    - Prepare and measure protocols
    - Entanglement based protocols
- Implementation
- Conclusion

Quantum Cryptography

- Uses properties of quantum mechanics to execute cryptographic tasks
  - Quantum Key Distribution

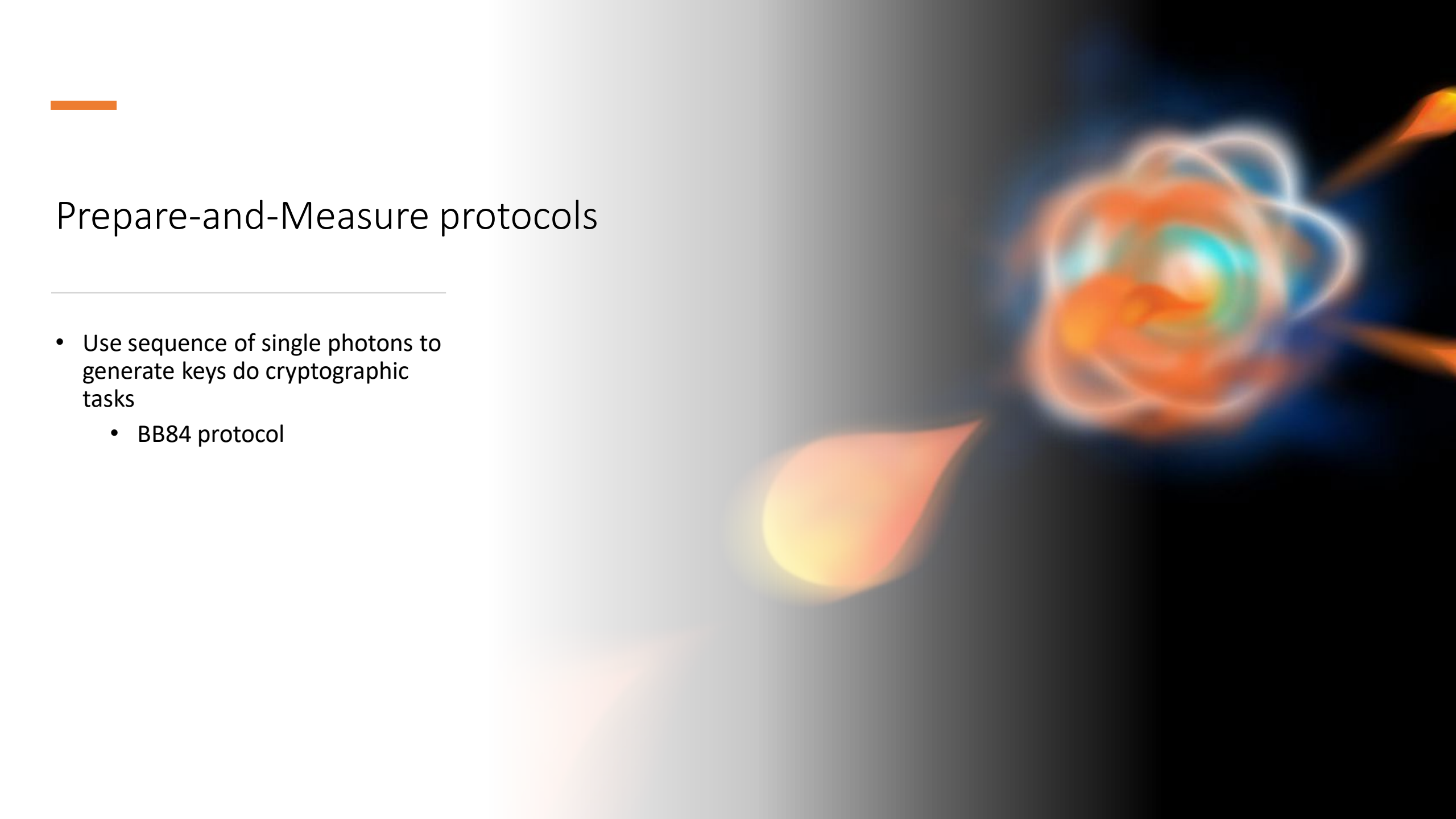
Quantum Key Distribution (QKD)

- Uses the Heisenberg's uncertainty principle
  - Reading data from quantum state changes the state
- Uses no cloning theorem
  - Copying data from quantum state destroys the state
- There are two types of (QKD) protocols
  - Prepare-and-Measure protocol
    - Uses sequence of single photons
  - Entanglement-Based protocol
    - Uses sequence of entangled photons



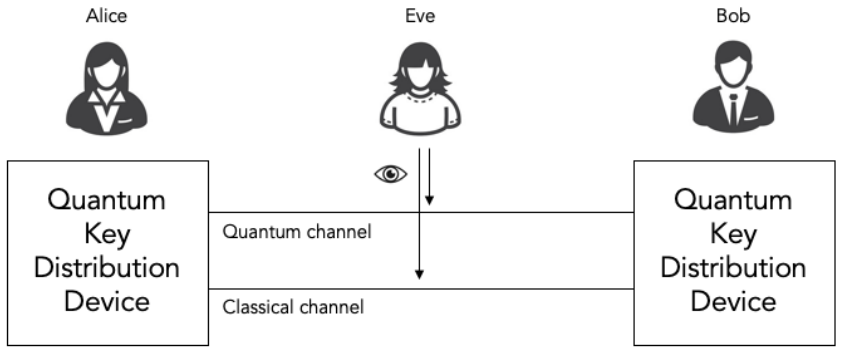
Prepare-and-Measure protocols

- Use sequence of single photons to generate keys do cryptographic tasks
  - BB84 protocol



BB84 Protocol

- BB84 protocol is used to generate random keys for two parties to use

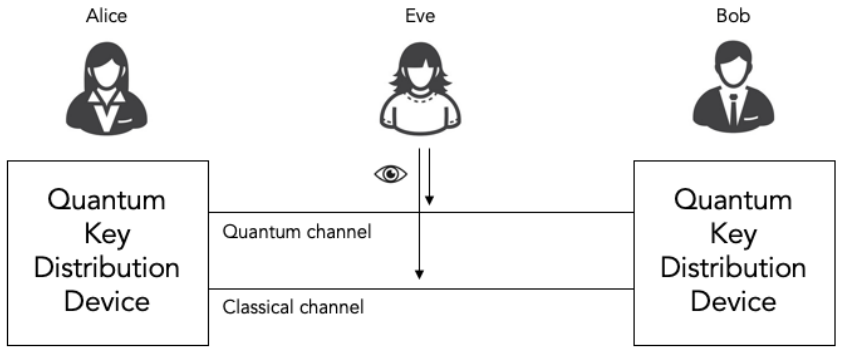


Y = Yes N = No R = Random

Alice's bits	1	1	0	1	0	1	0	1	1	0	1	0	0	1	1	0	1	0	0	1	0	1	1	1	1	0	0
Alice's basis (filter)	×	×	+	+	×	×	×	+	+	×	+	×	×	+	+	+	×	×	+	×	×	×	×	+	+	+	+
Bob's basis (filter)	+	+	×	×	×	×	+	+	+	×	×	+	+	+	×	+	+	×	+	×	+	×	×	+	+	+	+
Bob's bits after measurement	R	R	R	R	0	1	R	1	1	0	R	R	R	1	R	0	R	0	0	1	R	1	1	1	1	0	0
Same basis?	N	N	N	N	Y	Y	N	Y	Y	Y	N	N	N	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Bits to keep					0	1		1	1	0				1		0		0	0	1		1	1	1	1	0	0

BB84 Protocol

- BB84 protocol is used to generate random keys for two parties to use

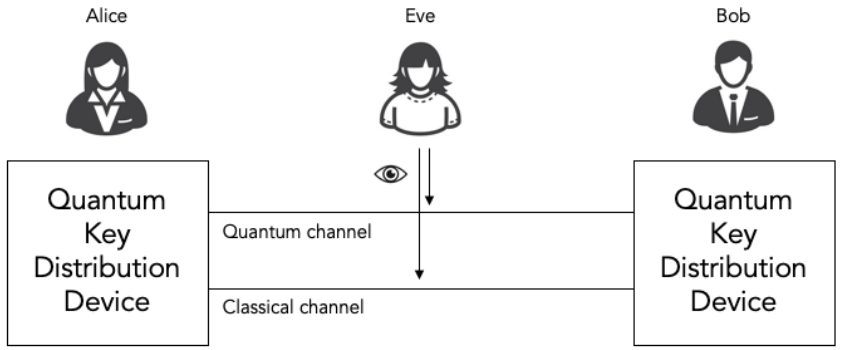


Y = Yes N = No R = Random

Alice's bits	1	1	0	1	0	1	0	1	1	0	1	0	0	1	1	0	1	0	0	1	0	1	1	1	1	0	0
Alice's basis (filter)	×	×	+	+	×	×	×	+	+	×	+	×	×	+	+	+	×	×	+	×	×	×	×	+	+	+	+
Bob's basis (filter)	+	+	×	×	×	×	+	+	+	×	×	+	+	+	×	+	+	×	+	×	+	×	×	+	+	+	+
Bob's bits after measurement	R	R	R	R	0	1	R	1	1	0	R	R	R	1	R	0	R	0	0	1	R	1	1	1	1	0	0
Same basis?	N	N	N	N	Y	Y	N	Y	Y	Y	N	N	N	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Bits to keep					0	1		1	1	0				1		0		0	0	1		1	1	1	1	0	0

BB84 Protocol

- BB84 protocol is used to generate random keys for two parties to use



Y = Yes N = No R = Random

Alice's bits	1	1	0	1	0	1	0	1	1	0	1	0	0	1	1	0	1	0	0	1	0	1	1	1	1	0	0
Alice's basis (filter)	×	×	+	+	×	×	×	+	+	×	+	×	×	+	+	+	×	×	+	×	×	×	×	+	+	+	+
Bob's basis (filter)	+	+	×	×	×	×	+	+	+	×	×	+	+	+	×	+	+	×	+	×	+	×	×	+	+	+	+
Bob's bits after measurement	R	R	R	R	0	1	R	1	1	0	R	R	R	1	R	0	R	0	0	1	R	1	1	1	1	0	0
Same basis?	N	N	N	N	Y	Y	N	Y	Y	Y	N	N	N	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Bits to keep					0	1		1	1	0				1		0		0	0	1		1	1	1	1	0	0

BB84 Protocol

Alice's bits	1	0	1	0	1	1	0	1	0	0	1	1	0	1	0	0	1	0	1	1	1	1	0	0
Alice's basis (filter)	+	×	×	×	+	+	×	+	×	×	+	+	+	×	×	+	×	×	×	×	+	+	+	+
Bob's basis (filter)	×	×	×	+	+	+	×	×	+	+	+	×	+	+	×	+	×	+	×	×	+	+	+	+
Bob's bits after measurement	R	0	1	R	1	1	0	R	R	R	1	R	0	R	0	0	1	R	1	1	1	1	0	0
Same basis?	N	Y	Y	N	Y	Y	Y	N	N	N	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Bits to keep		0	1		1	1	0				1		0		0	0	1		1	1	1	1	0	0

Character	**Binary**
H	01001000
I	01001001

Message 01001000 01001001

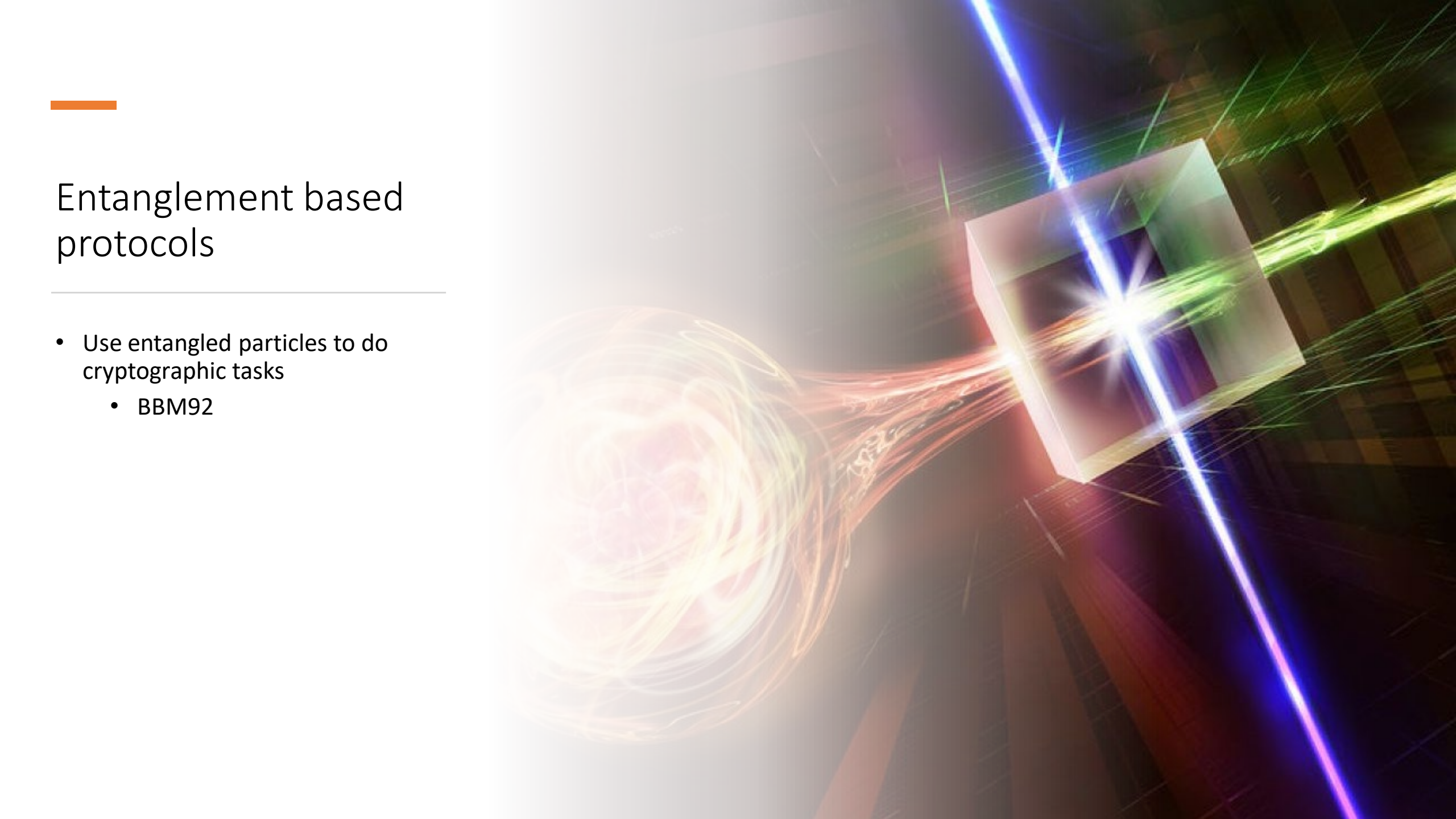
⊕

Key 01110100 01111100

Ciphertext 00101100 00110101

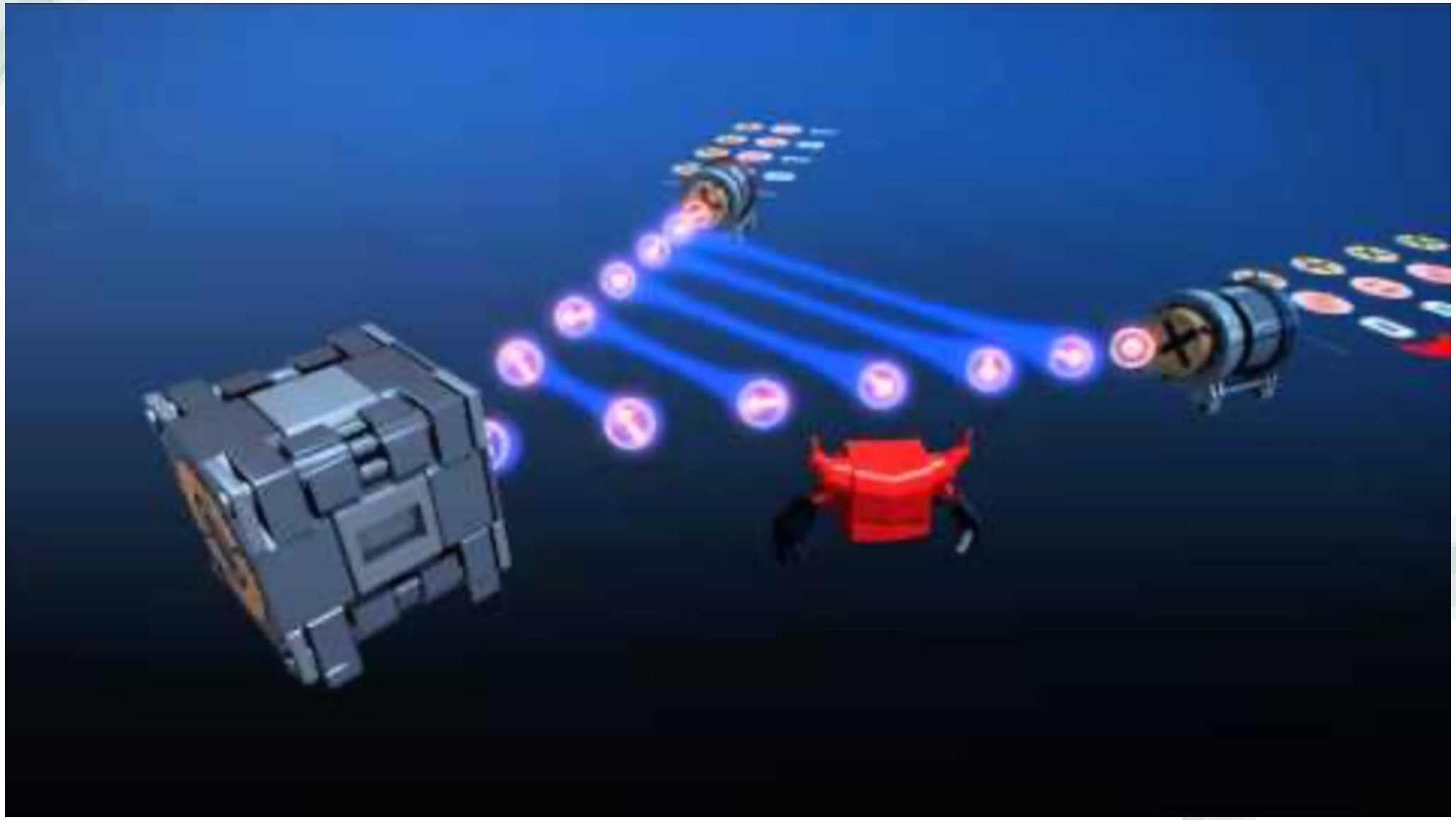
Entanglement based protocols

- Use entangled particles to do cryptographic tasks
  - BBM92



Entanglement based protocol

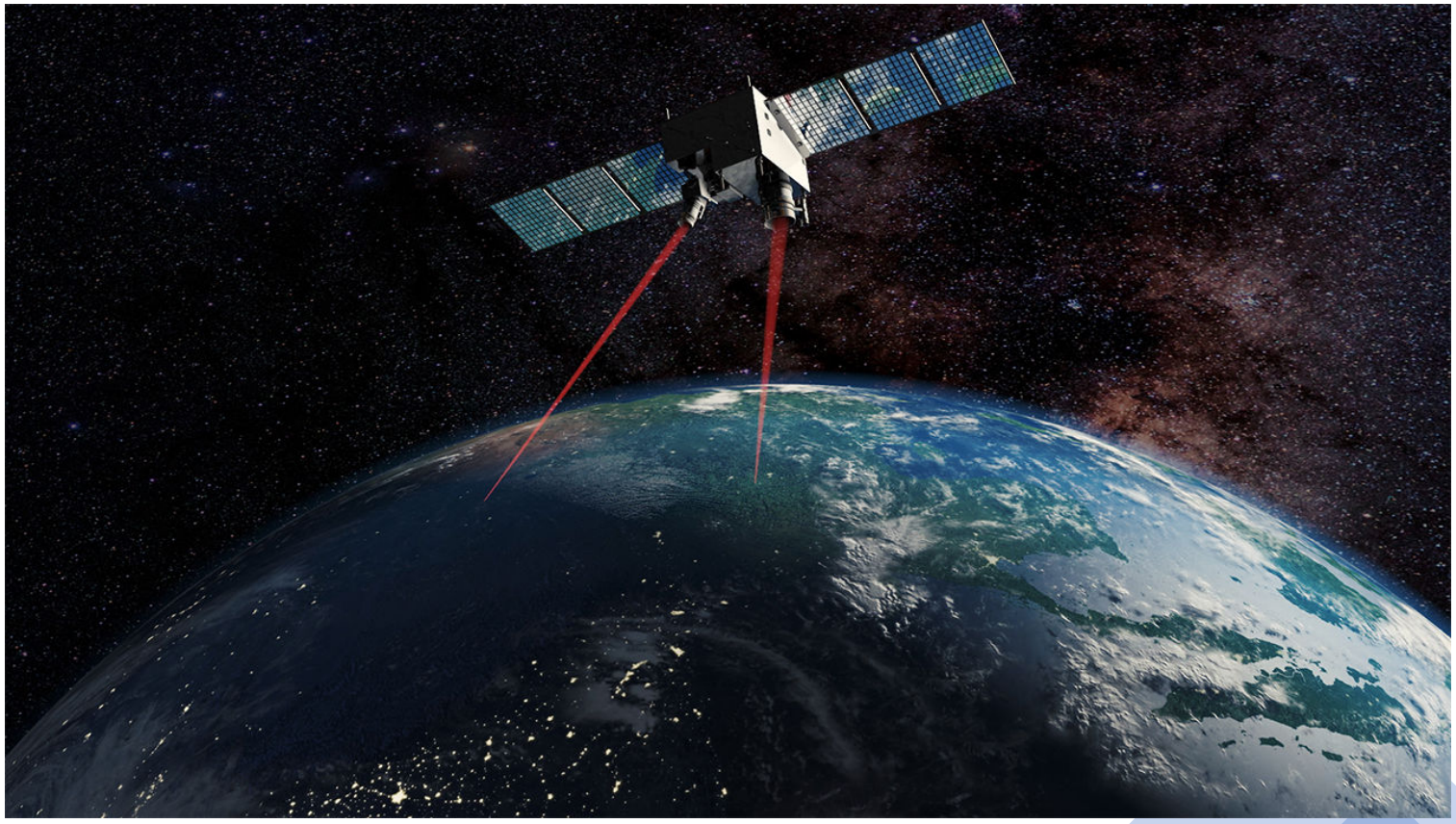
- BBM92 uses entangled photons to generate random keys



Implementation

Entanglement-based QKD has been achieved using satellites

- Ground stations were 1,120 kilometers apart
- High efficiency telescopes were used



Outline

- Introduction ✓
- Background ✓
- Quantum cryptography ✓
  - Quantum key distribution
    - Prepare and measure protocols
    - Entanglement based protocols
- Implementation ✓
- Conclusion

Conclusion

- Quantum key distribution protocols are very promising technologies that can enable us to create unbreakable encryptions
- Some implementations are available commercially
- There is still a lot more that needs to be done to implement them

Acknowledgments

Thank you to Elena Machkasova for making this talk possible

Thank you to all my family and friends

References

- D. Bruss, G. Erď elyi, T. Meyer, T. Riege, and J. Rothe. Quantum cryptography: A survey. ACM Comput. Surv., 39(2):6–es, July 2007
- Christof Paar & Jan Pelzl. Understanding Cryptography. Springer Science and Business Media, 2009.
- V. Mavroeidis, K. Vishi, M. D. , and A. Jøsang. The impact of quantum computing on present cryptography. International Journal of Advanced Computer Science and Applications, 9(3), 2018.
- J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G.Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li,Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y.Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He,Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C.Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z.Peng, J.-Y. Wang, and J.-W. Pan. Satellite-based entanglement distribution over 1200 kilometers. Science, 356(6343):1140–1144, 2017
- S. Wang, M. Rohde, and A. Ali. Quantum cryptography and simulation: Tools and techniques. In Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy, ICCSP 2020,page 36–41, New York, NY, USA, 2020. Association for Computing Machinery
- W. Jia, Y. Zhang, H. Yu, and Y. Bian. A quantum key distribution protocol based on ldpc error correcting codes. In Proceedings of the ACM Turing Celebration Conference - China, ACM TURC ’19, New York, NY,USA, 2019. Association for Computing Machinery

Picture and Video References

- https://securitybrief.com.au/story/department-defence-invest-326m-quantum-key-research
- https://newatlas.com/physics/new-distance-record-quantum-entanglement-light-matter/
- https://www.youtube.com/watch?v=LaLzshIosDk&feature=emb_title
- https://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance
- http://royaltots.sch.id/kids-codes-and-computer/

Questions