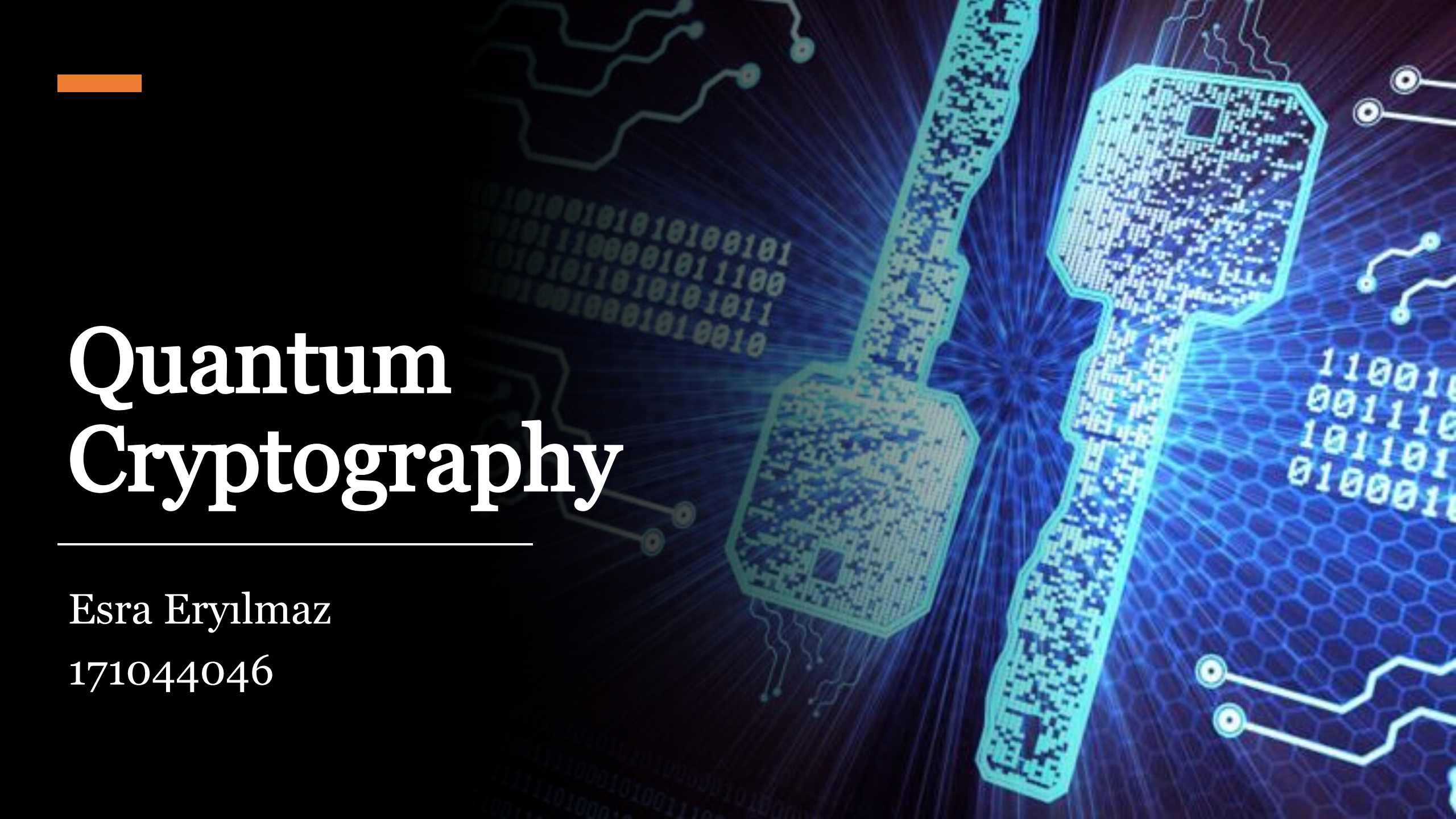
Quantum Cryptography

Esra Eryılmaz
171044046



Content

- What is cryptography?
- What is quantum cryptography?
- History
- Quantum cryptography explanation.
- Conclusion
- Bibliography

What is cryptography?

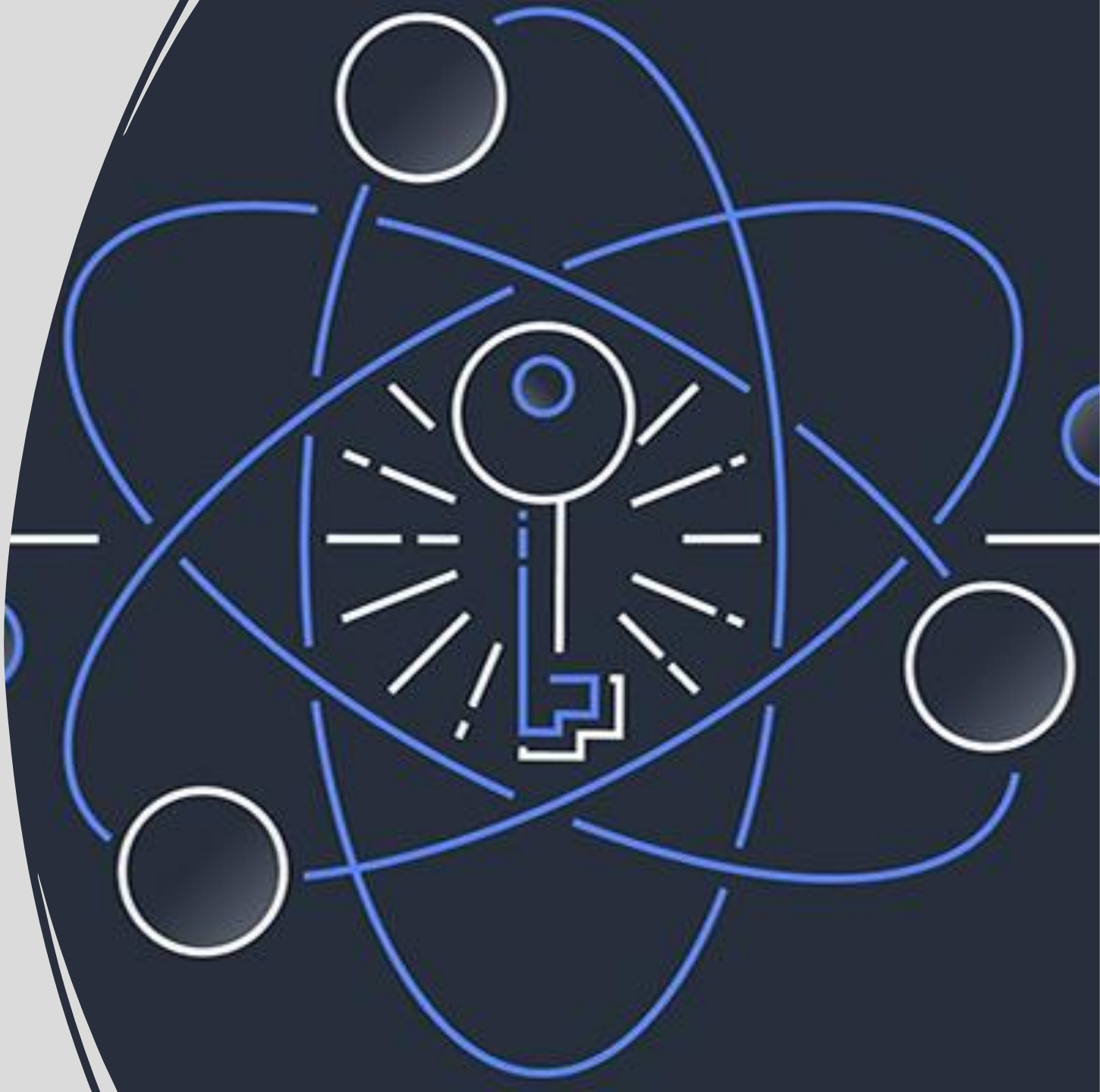
Cryptography is the art of devising codes and ciphers.

Crypto analysis is the art of breaking them.

Cryptology is the combination of the two i.e Cryptography and Crypto analysis.

What is quantum cryptography?

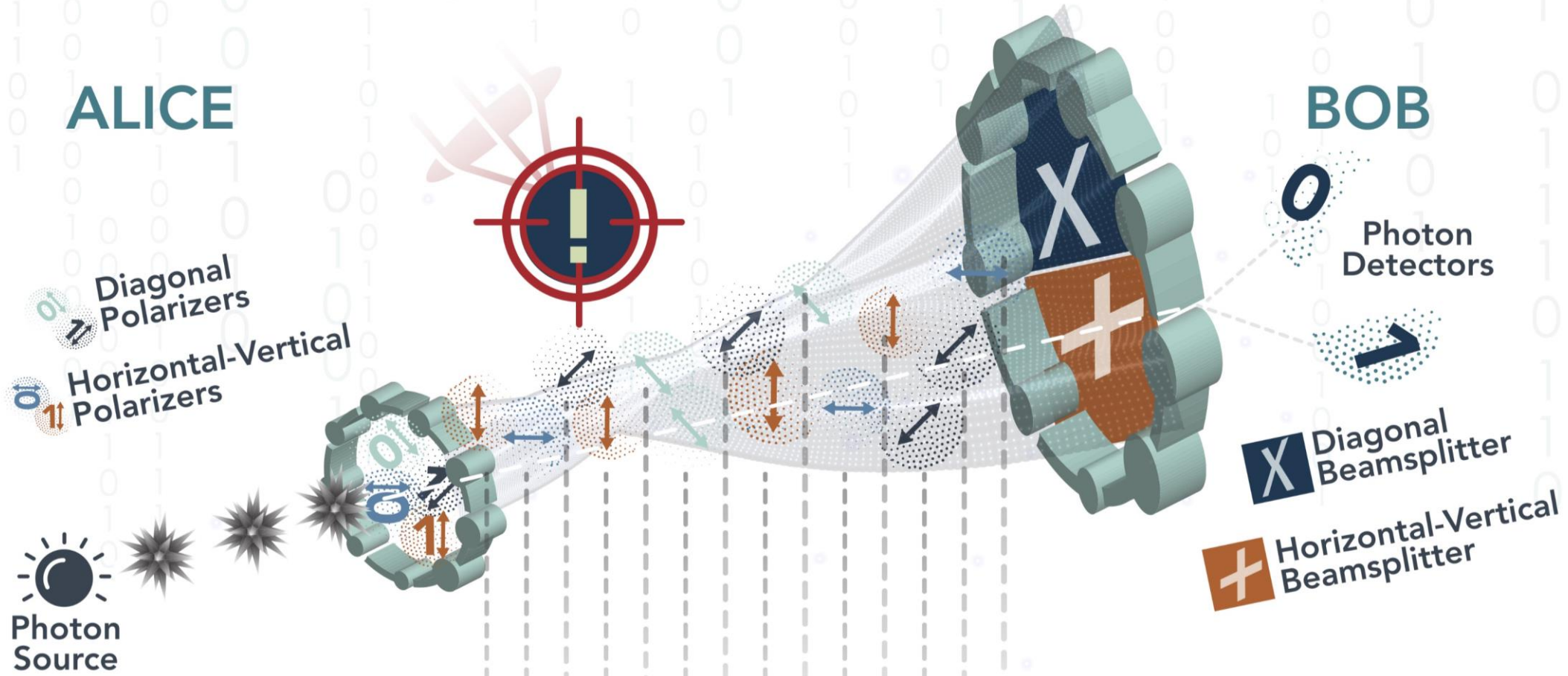
- Quantum cryptography is a science that applies quantum mechanics principles to data encryption and data transmission so that data cannot be accessed by hackers – even by those malicious actors that have quantum computing of their own.



History

- Quantum cryptography attributes its beginning by the work of Stephen Wiesner and Gilles Brassard. In the early 1970s, Wiesner, then at Columbia University in New York, introduced the concept of quantum conjugate coding. His seminal paper titled "Conjugate Coding" was rejected by the IEEE, but was eventually published in 1983 in SIGACT News.
- In this paper he showed how to store or transmit two messages by encoding them in two "conjugate observables", such as linear and circular polarization of photons, so that either, but not both, of which may be received and decoded.

QUANTUM CRYPTOGRAPHY EXPLAINED



Alice's Bit Sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0	
	+	X	+	+	X	X	+	+	X	+	X	X	+	+	Bob's Detection
	1	0	0	1	0	0	1	1	0	0	0	1	0	0	Bob's Measurements
Sifted Key	1	–	–	1	0	0	–	1	0	0	–	1	–	0	Sifted Key

Conclusion

- Quantum cryptography promises to revolutionize secure communication by providing security based on the fundamental laws of physics, instead of the current state of mathematical algorithms or computing technology.
- The devices for implementing such methods exist and the performance of demonstration systems is being continuously improved.
- Within the next few years, if not months, such systems could start encrypting some of the most valuable secrets of government and industry.

Bibliography

- Bennett, Charles H., et al. "Quantum cryptography, or unforgeable subway tokens." Advances in Cryptology. Springer, Boston, MA, 1983.
- Pirandola, Stefano, et al. "Advances in quantum cryptography." Advances in optics and photonics 12.4 (2020): 1012-1236.
- Broadbent, Anne, and Christian Schaffner. "Quantum cryptography beyond quantum key distribution." Designs, Codes and Cryptography 78.1 (2016): 351-382.
- Chen, Lily, et al. Report on post-quantum cryptography. Vol. 12. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology, 2016.
- Bernstein, Daniel J., and Tanja Lange. "Post-quantum cryptography." Nature 549.7671 (2017): 188-194.
- Tomamichel, Marco, et al. "Tight finite-key analysis for quantum cryptography." Nature communications 3.1 (2012): 1-6.
- Elliott, Chip. "Quantum cryptography." IEEE security & privacy 2.4 (2004): 57-61.
- https://www.techtarget.com/searchsecurity/definition/quantum-cryptography
- https://en.wikipedia.org/wiki/Quantum_cryptography

- ***thank you for listening to my presentation i hope u enjoyed!***