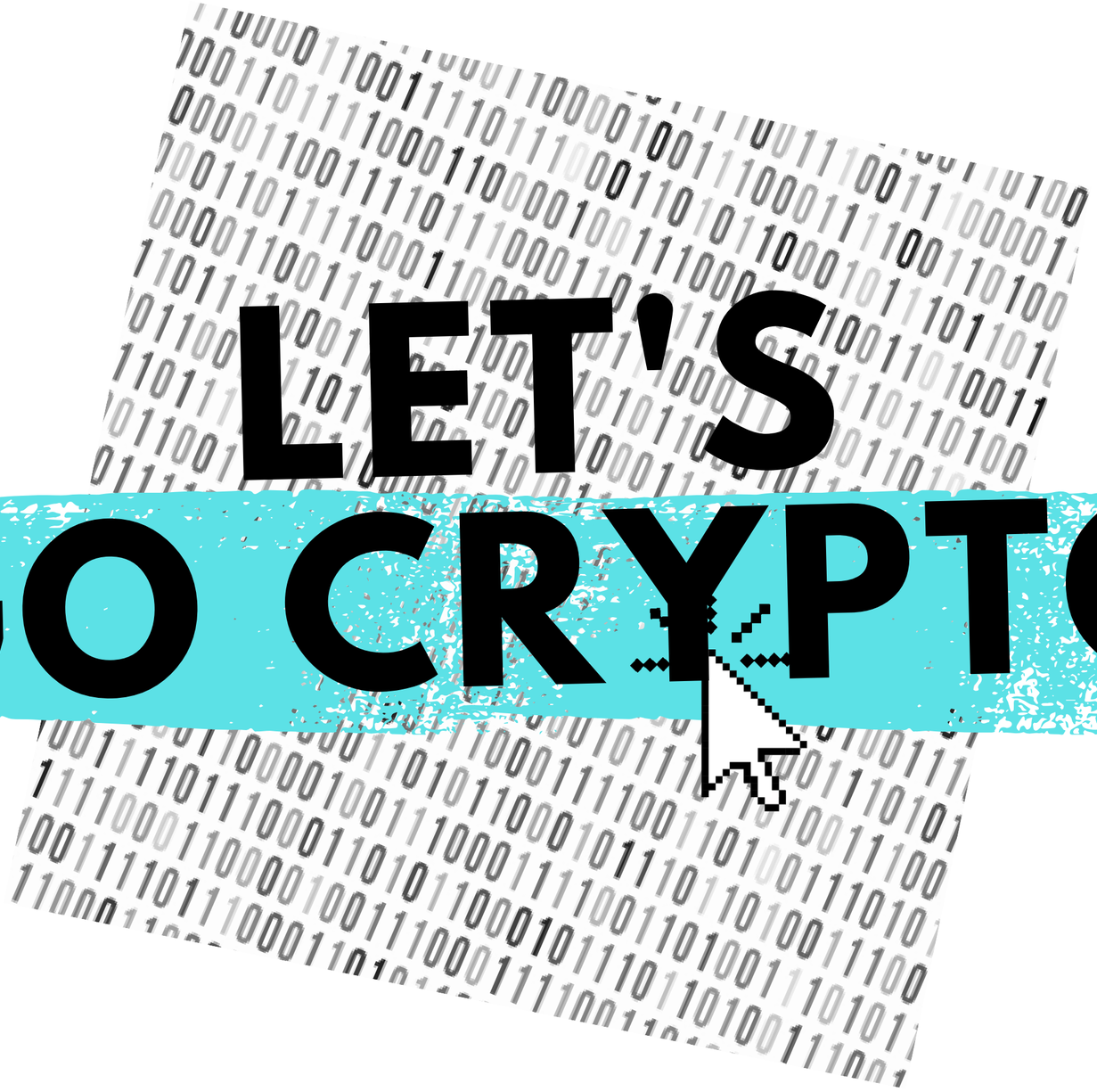
LET'S GO CRYPTO



EXPLORING QUANTUM THEORY WITH QUBITS

AUTHOR: DENISA VÍTKOVÁ

MAY 6, 2022

CRYPTOGRAPHY

the art and science to secure our communication in the insecure world

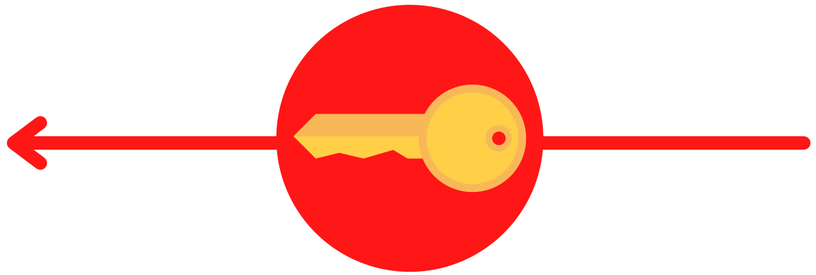
SYMMETRIC encryption

PLAINTEXT

This is some random text which is not encrypted and can be read by anyone.

encryption

SECRET KEY



decryption

CIPHERTEXT

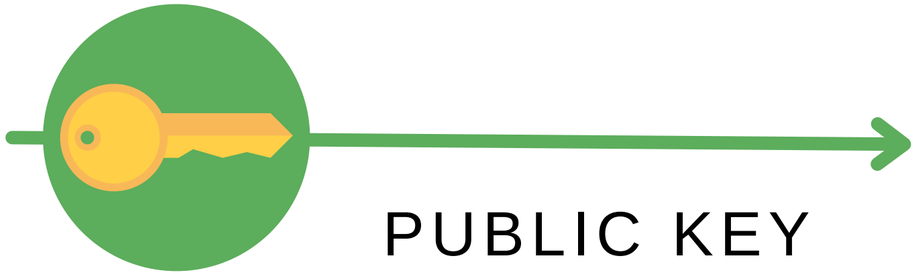
G$f; f; ;bzr e#?ubz grkg j$fp§ v; ?bg r?pelcgru #au p#? or er#u ol #?lb?r.

ASYMMETRIC encryption

PLAINTEXT

This is some random text which is not encrypted and can be read by anyone.

encryption



PUBLIC KEY

PRIVATE KEY

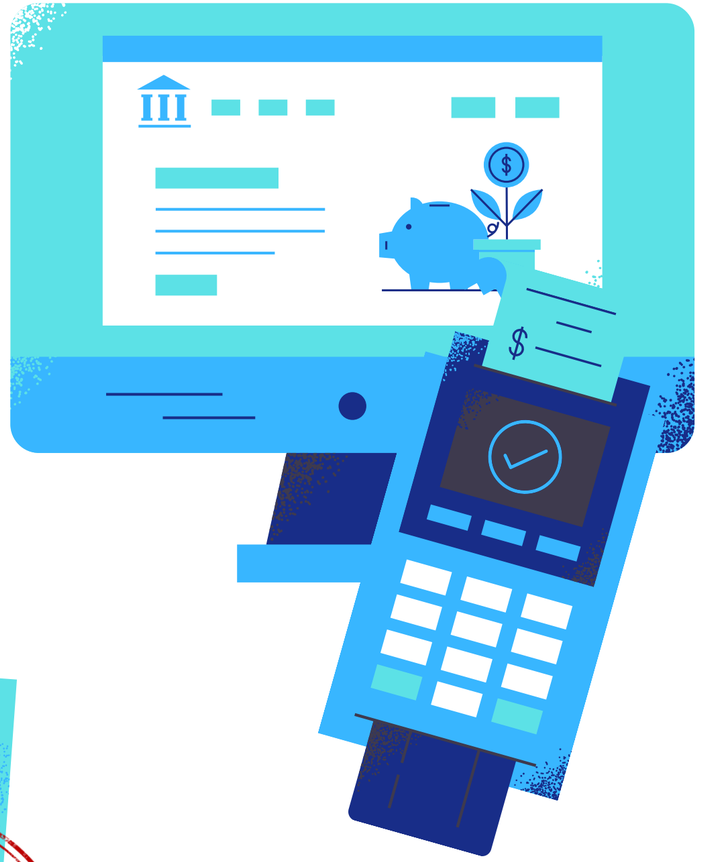
decryption

CIPHERTEXT

G$f; f; ;bzr e#?ubz grkg j$fp§ v; ?bg r?pelcgru #au p#? or er#u ol #?lb?r.

accessing your bank account

making online transactions



sending private messages (with business plans :D)

computer passwords

CRYPTOGRAPHY

SYMMETRIC cipher

one-time pad
safest – in principle indecipherable
needs a large codebook
AES

! **stolen codebook issue**

ASYMMETRIC cipher

private + public key
encryption with a public key
decryption with a private key
RSA and elliptic curves

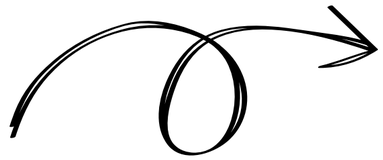
! **stolen private key issue**

preventing eavesdropping

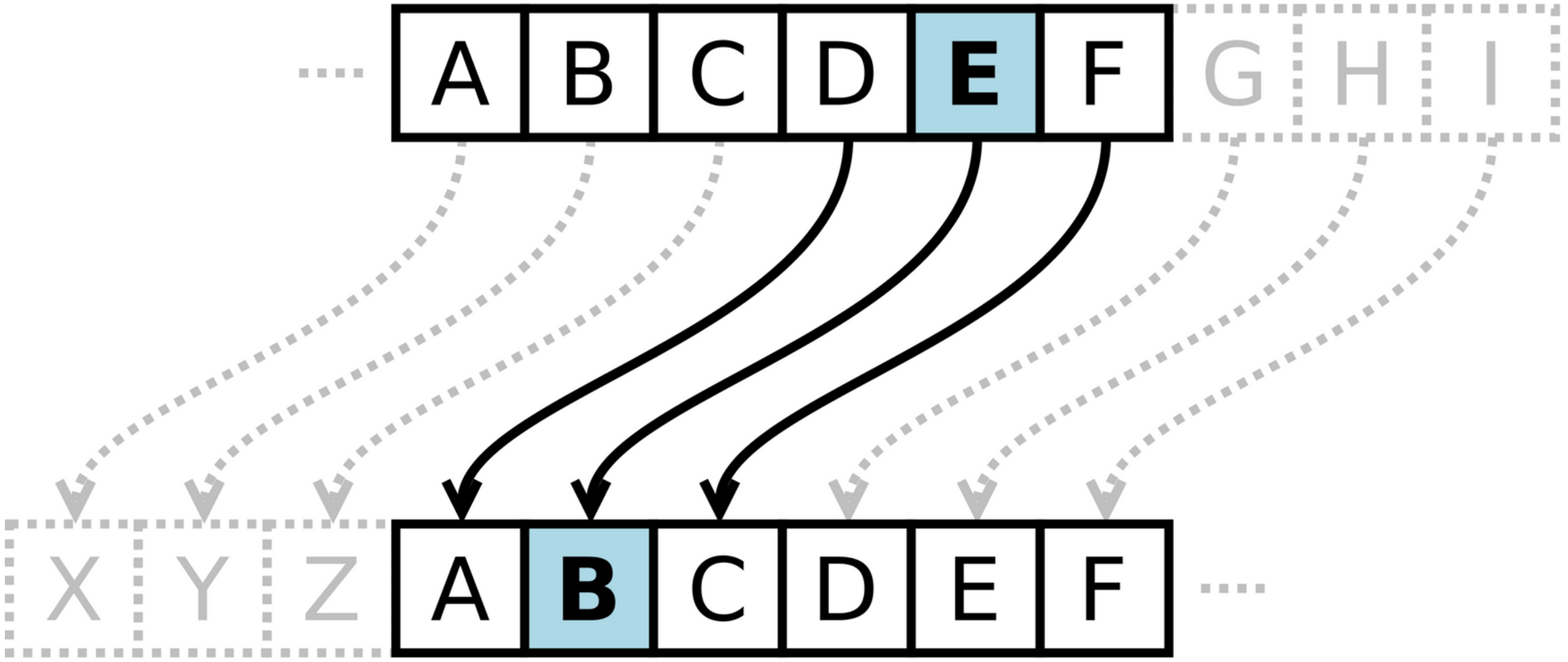
encryption of the data

verification of the sender

electronic signatures



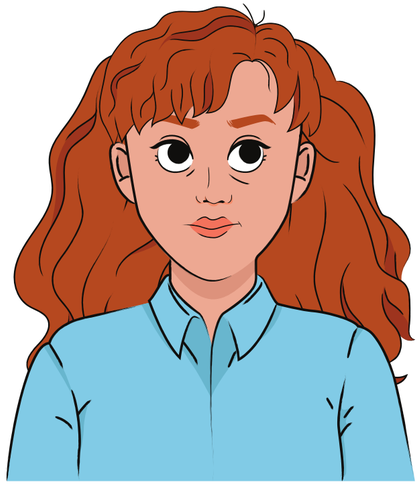
CLASSIC CRYPTOGRAPHY



ALPHABET SHIFT CIPHER

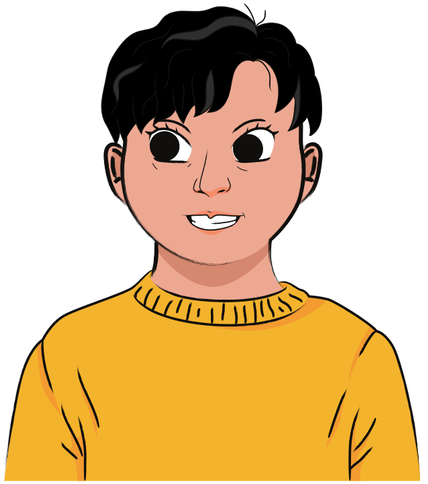
ROT13 double encryption

Why is it
really "safe"?



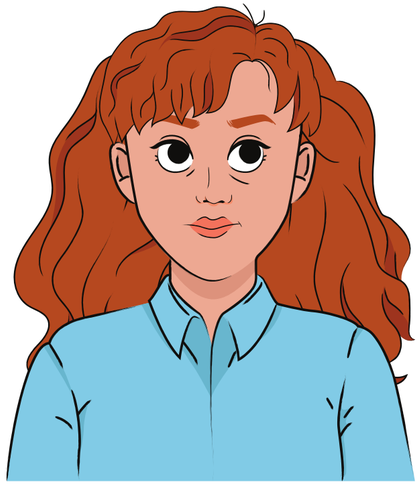
ALICE

series of bits to be sent to Bob

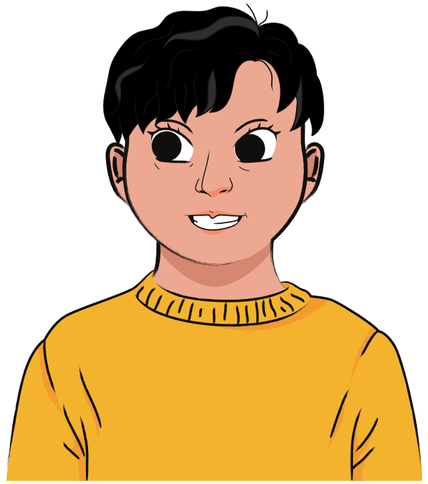


BOB

EVE (eavesdropper)



series of bits to be sent to Bob

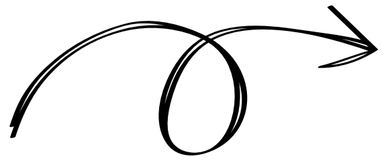


ALICE

BOB

modified (Alice's) message

TRUDY (intruder)



POST-QUANTUM CRYPTOGRAPHY

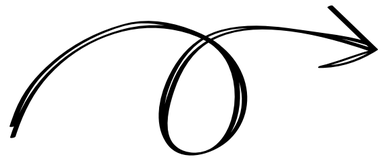
POST-QUANTUM CRYPTOGRAPHY

refers to cryptographic algorithms (usually public-key algorithms) that we think are secure enough to withstand a cryptanalytic attack by a quantum computer

- the integer factorization problem
- the discrete logarithm problem
- the elliptic-curve discrete logarithm problem

We can easily solve all of these problems on a powerful enough quantum computer running

SHOR'S ALGORITHM



QUANTUM CRYPTOGRAPHY

SUMMARY of QM used in Q-CRYPTOGRAPHY

1.

The particles that make up the universe are **inherently uncertain** and can simultaneously exist in more than one place or more than one state of being.

2.

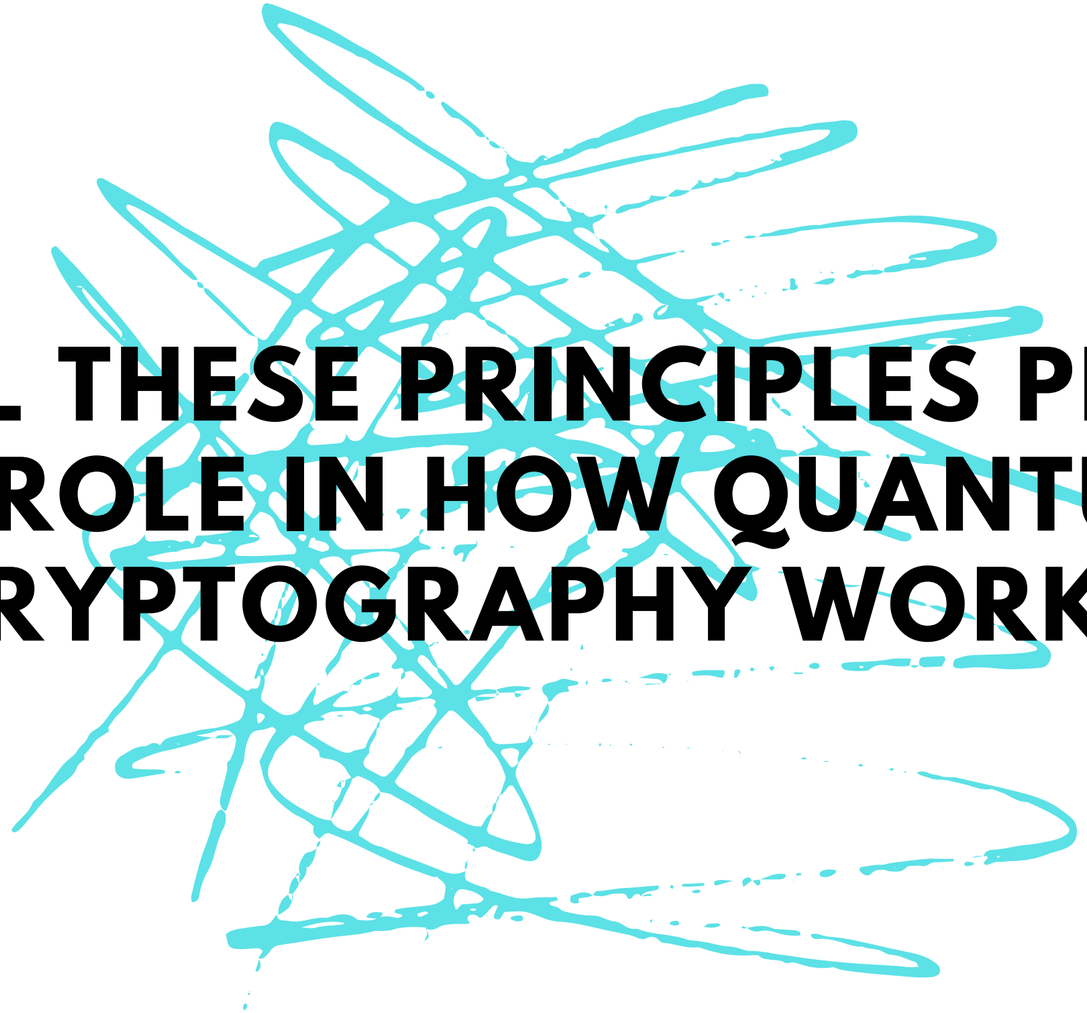
Photons are **generated randomly** in one of two quantum states.

3.

It is **not possible to measure** a quantum property without altering or disturbing it.

4.

We can make a copy of some quantum properties of a particle, but **not of the whole** particle.



ALL THESE PRINCIPLES PLAY A ROLE IN HOW QUANTUM CRYPTOGRAPHY WORKS.

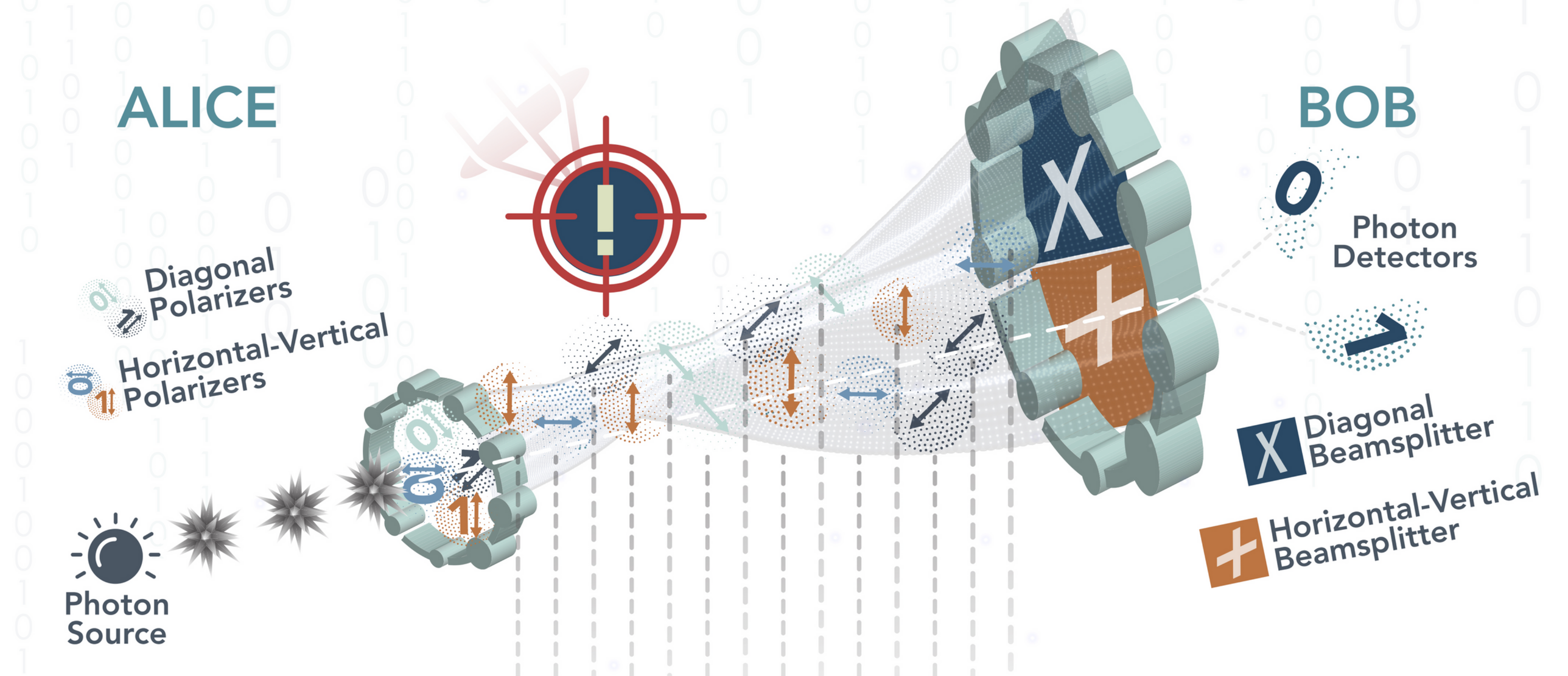
QUANTUM CRYPTOGRAPHY

sometimes as QKD (Quantum Key Distribution)

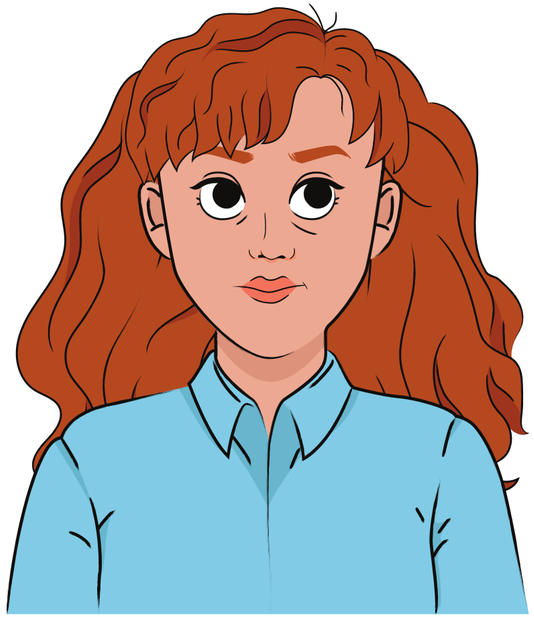
uses principles of quantum mechanics to encrypt data

data are sent in form of photons, not bits

"VIRTUALLY UNHACKABLE"



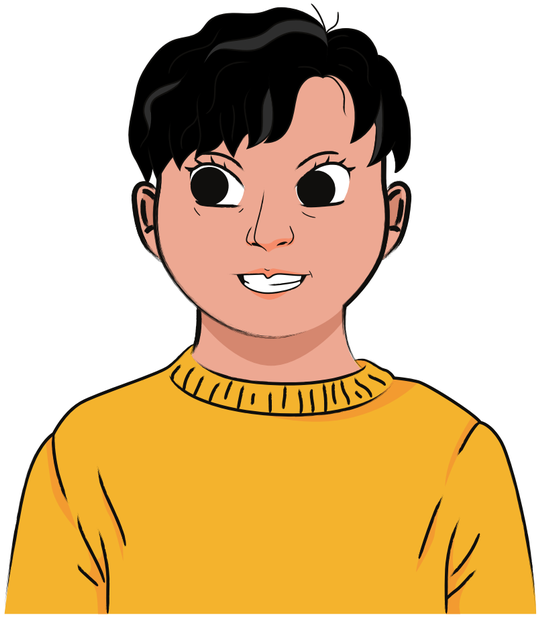
Alice's Bit Sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0		
	+	X	+	+	X	X	+	+	X	+	X	X	+	+	Bob's Detection	
	1	0	0	1	0	0	1	1	0	0	0	1	0	0	Bob's Measurements	
Sifted Key	1	–	–	1	0	0	–	1	0	0	–	1	–	0	Sifted Key	



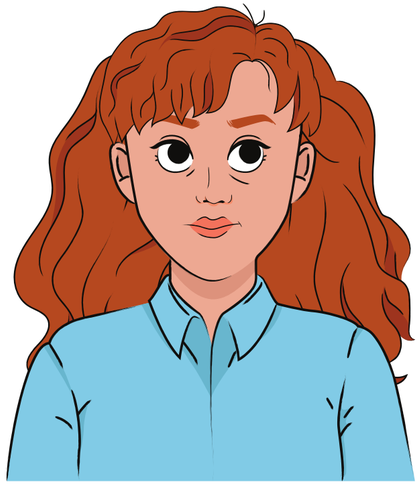
ALICE

polarized photons for Bob

polarized photons for Alice

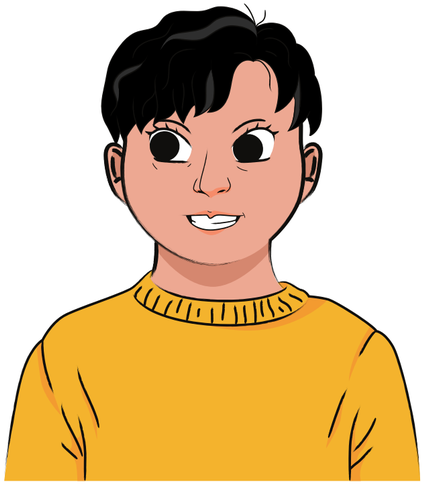


BOB



ALICE

a series of polarized photons for Bob

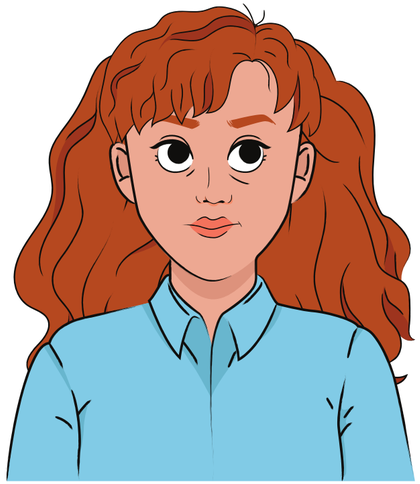


BOB

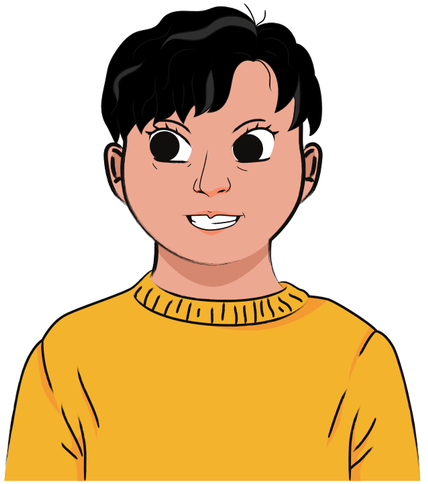
EVE (eavesdropper)

WHERE IS THE PROBLEM?

Share your opinions!



a series of polarized photons for Bob

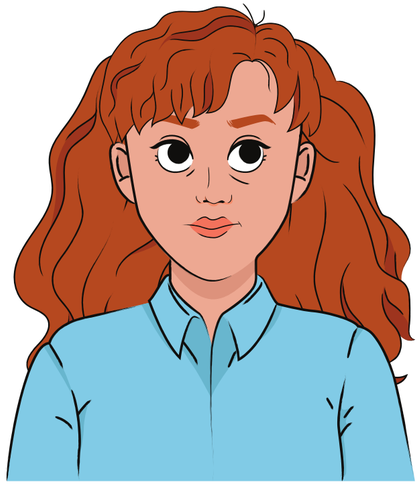


ALICE

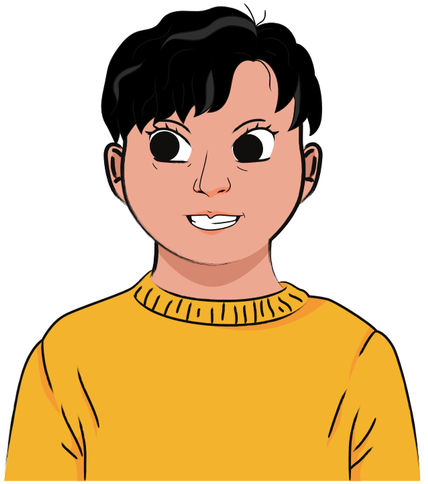
BOB

a copy of polarized photons

EVE (eavesdropper)



a series of polarized photons for Bob



ALICE

a copy of polarized photons

BOB

EVE (eavesdropper)

NO READING, NO CLONING

By reading the photon, Eve changes the quantum state of the proton.

Moreover, there is no possibility to clone the state and then read it.

POSSIBLE ATTACKS IN QC

Photon Number Splitting (PNS) Attack

Some photons from a pulse can be captured by Eve, Eve uses the same polarizer as Bob and gets the key without being detected.

Faked-State Attack

Eve uses a copy of Bob’s photon detector, captures the photons intended for Bob and further passes them to him. Eve knows about the encoded bit, Bob thinks that he received it from Alice.

RESOURCES

Crawley, K. (2019, July 17). **Quantum computing threatens all current cryptography.** Venafi. Retrieved May 2, 2022, from https://www.venafi.com/blog/quantum-computing-threatens-all-current-cryptography

Quantum cryptography, explained. Quantum Xchange. (2022, March 22). Retrieved May 2, 2022, from https://quantumxc.com/blog/quantum-cryptography-explained/

Wootters, W. K., & Zurek, W. H. (2009, February 1). **The no-cloning theorem.** Physics Today. Retrieved May 2, 2022, from https://physicstoday.scitation.org/doi/10.1063/1.3086114

Tóth, G. (2021, February). **No-cloning theorem and related issues.** Lecture. Retrieved May 2, 2022, from https://www.gtoth.eu/Transparencies/QINF_Nocloning_2021.pdf

Tamaki, K., & Lo, H.-K. (2005, May 24). **Quantum Key Distribution: Beyond No-Cloning Theorem.** arXiv. Retrieved May 2, 2022, from https://arxiv.org/pdf/quant-ph/0412035v3.pdf

Wikipedia contributors. (2022, April 28). **Post-quantum cryptography.** Wikipedia, The Free Encyclopedia. Retrieved May 2, 2022, from https://en.wikipedia.org/wiki/Post-quantum_cryptography

Wikipedia contributors. (2022, April 22). **Quantum cryptography.** Wikipedia, The Free Encyclopedia. Retrieved May 2, 2022, from https://en.wikipedia.org/wiki/Quantum_cryptography

Quantum cryptography. GeeksforGeeks. (2021, November 5). Retrieved May 3, 2022, from https://www.geeksforgeeks.org/quantum-cryptography/

Ling, A., Gerhardt, I., Lamas-Linares, A., & Kurtsiefer, C. (n.d.). **Practical Quantum cryptography and possible attacks.** Lecture, Berlin. Retrieved May 3, 2022, from https://media.ccc.de/v/24c3-2275-en-quantum_cryptography_and_possible_attacks, http://qolah.org/cryptoplay/24c3_qkd.pdf, https://www.slideshare.net/arinto/quantum-cryptography-and-possible-attacks

THANK YOU

FRIENDLY TALK ON A TOPIC

TIME FOR QUESTIONS