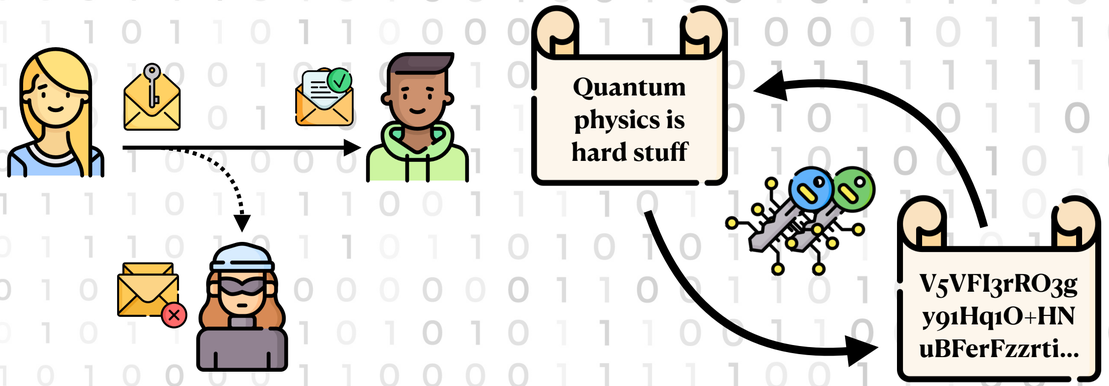
Dear Alice, it's Bob

An Introduction to QKD

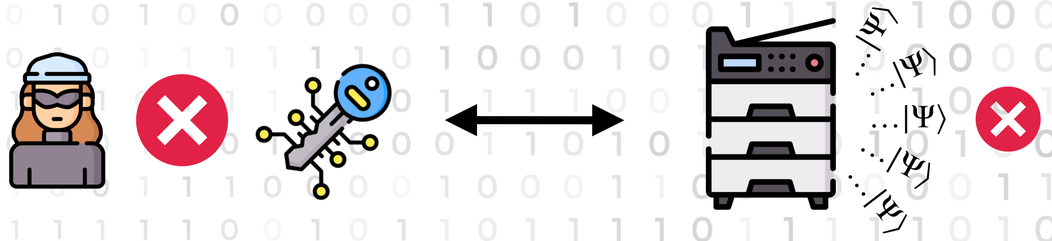
G.Rodari - PhD Seminars - 23/11

Outline

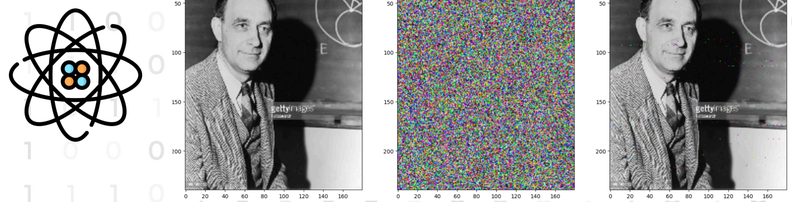
1. An introduction to (classical) **cryptography**



2. Let's go **quantum:** securing ***key distribution***

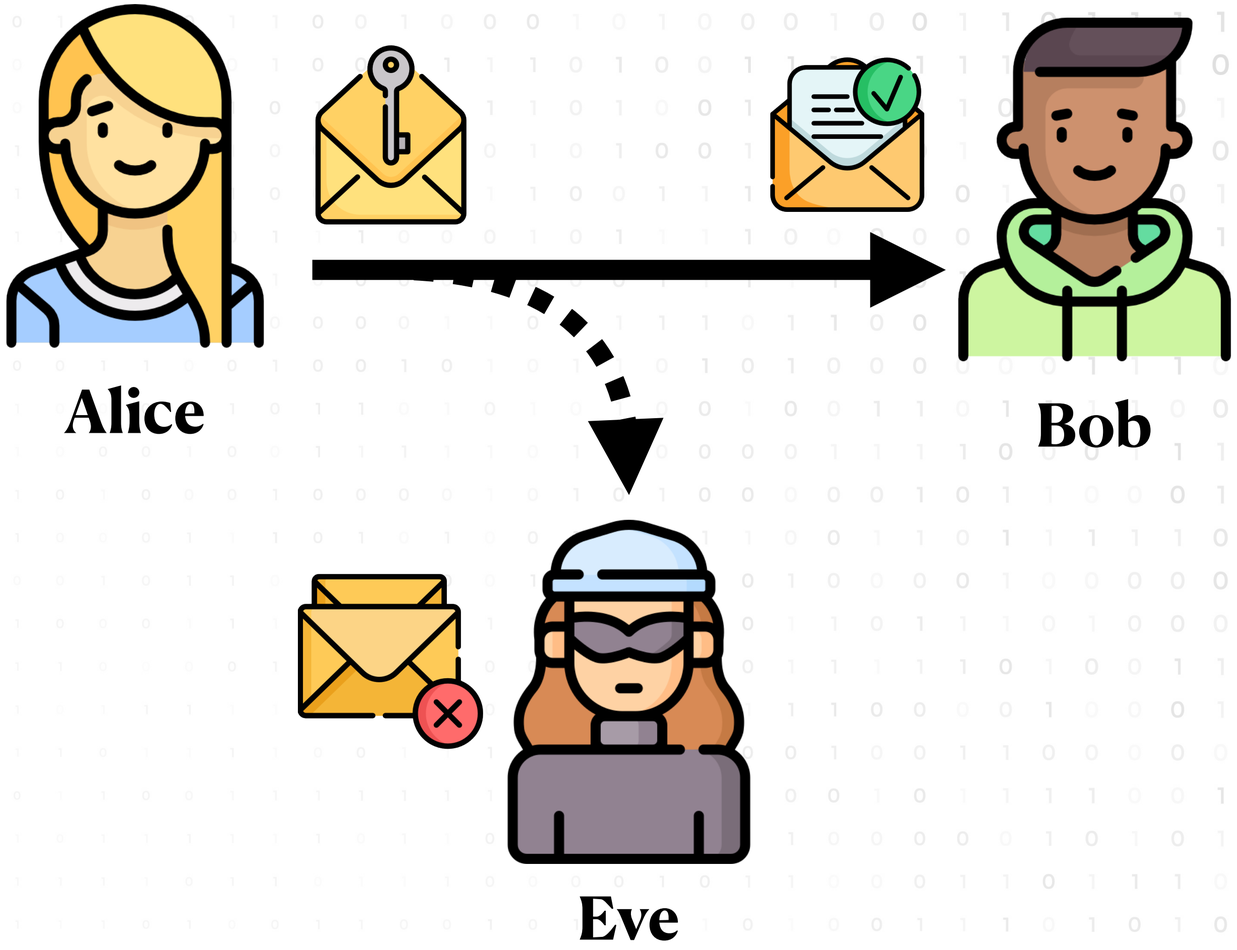


3. A concrete example: the **BB84** protocol



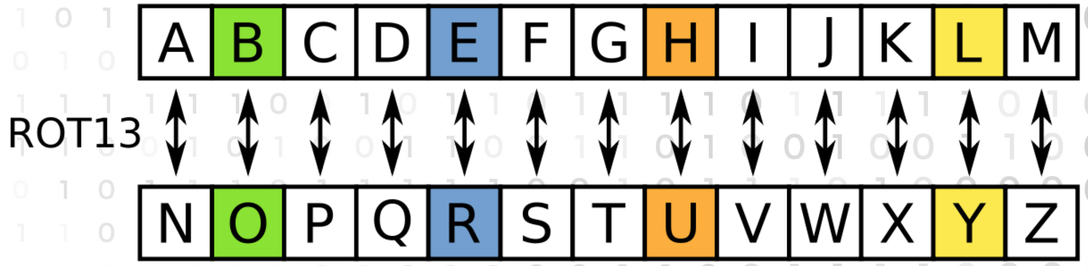
What is Cryptography?

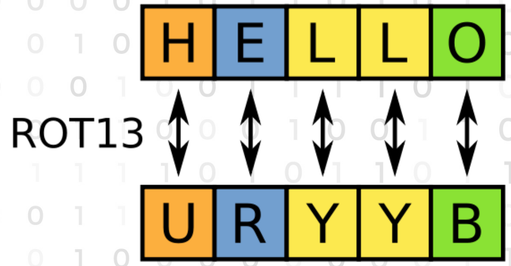
The ***science*** of hiding information from ***unwanted*** adversaries



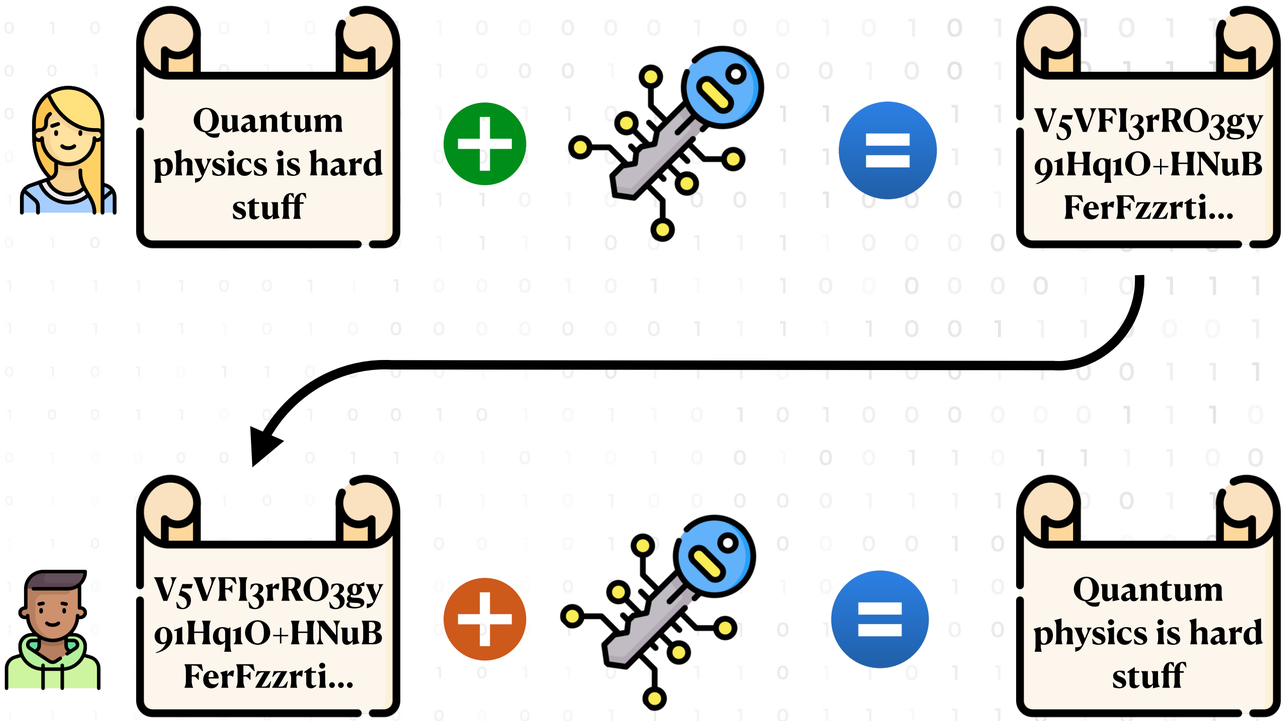
A simple example:

"Encrypt by substitution"





How does it work?



$E_{K_A}(M) = C$

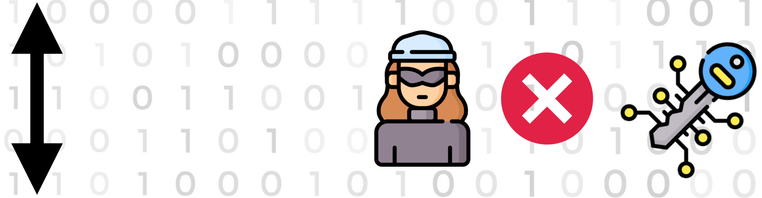
Encryption

$D_{K_B}(C) = M$

Decryption

- $K_A = K_B$: **symmetric** cryptography

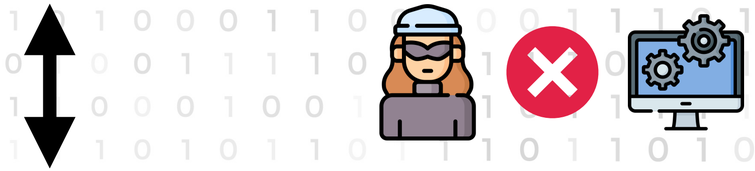
Unconditional security



Key is kept safe from Eve

- $K_A \neq K_B$: **asymmetric** cryptography

Secure as of today*



$E_K(M)$ is "**hard**" enough to invert

One Time Pad

XOR operation

Message: CIAO — 01000011 01001001 01000001 01001111

Key: DOGE — 01000100 01001111 01000111 01000101

00000111 00000110 00000110 00001010

01000100 01001111 01000111 01000101

Encrypted:FWGS

Key: DOGE

01000011 01001001 01000001 01001111

Message: CIAO

Unconditional Security

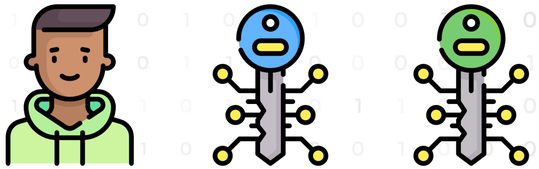
1) Key must be a **truly random** sequence
2) Each key can only be used **one time**
3) The key must be **secretly** distributed

Key Distribution problem

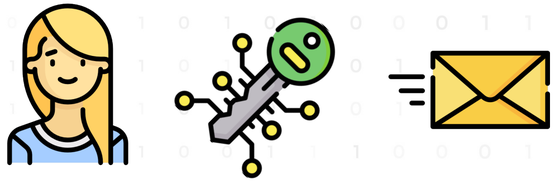
F.Miller (1842–1925)

G.Vernam (1890-1960)

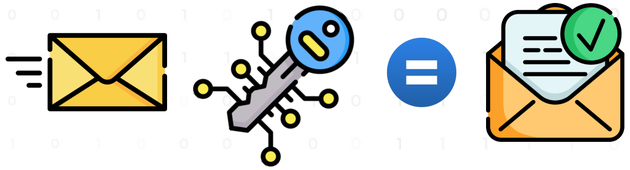
A Public Key system



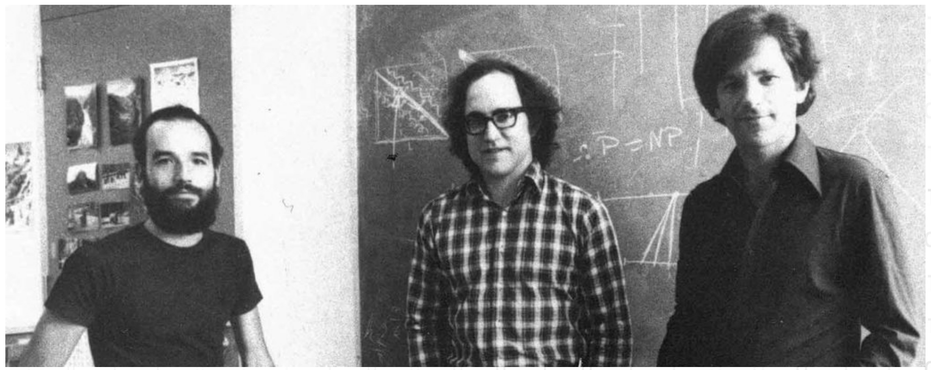
Bob produces a ***pair*** of keys: **Private** key and a **Public** key



Alice only needs the **Public** key to encrypt the message



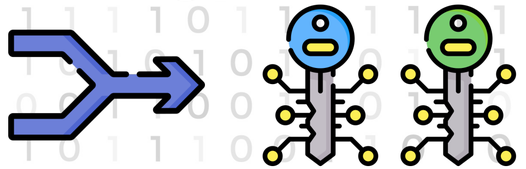
Message recovered **only** knowing the **Private** key



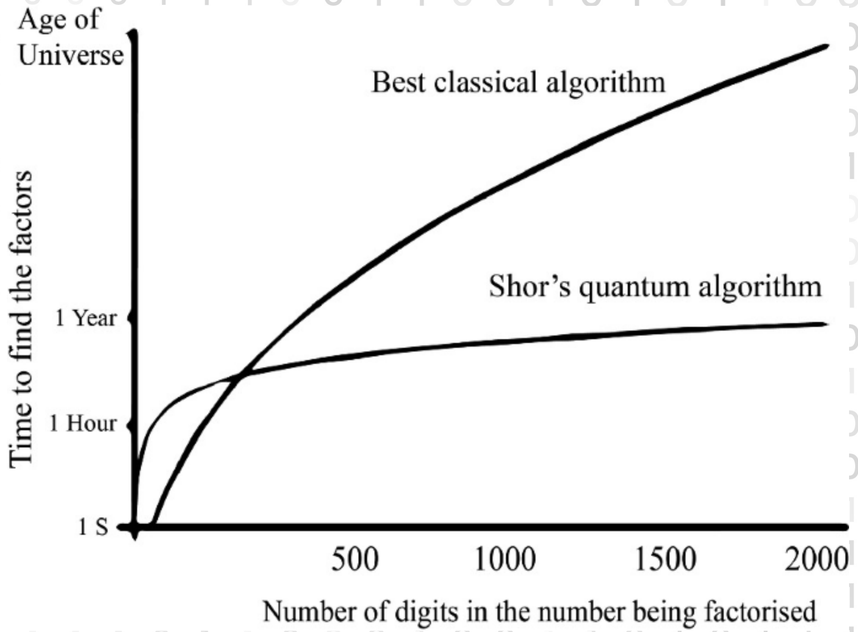
RSA: Rivest–**S**hamir–**A**dleman

Key pair depends on **big prime numbers**

$$n = pq$$



RSA security = **Hardness** of factorisation

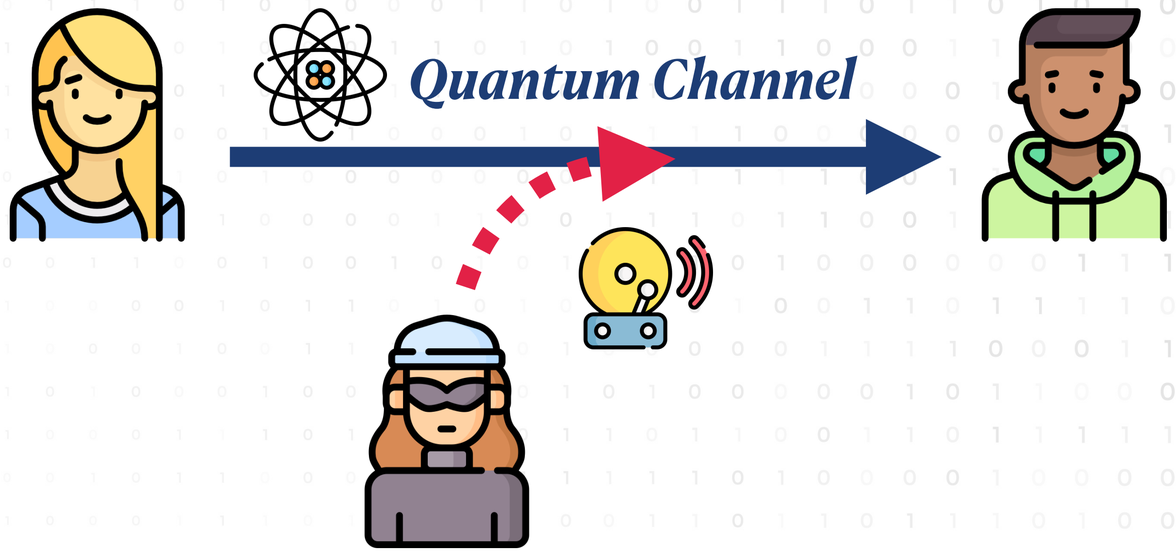


RSA is not **Quantum Proof**

Quantum Key Distribution

Review: Arxiv:quant-ph/0101098

What if one can use **Quantum Mechanics** to **securely** distribute a key?

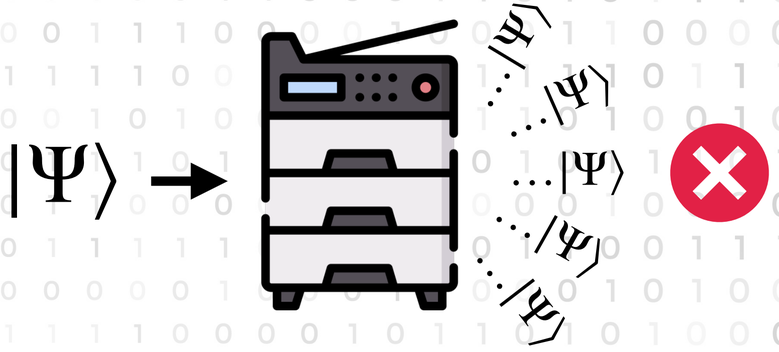


To gain information on the "quantum" key:

1) Eve must **observe** a quantum system
2) When observed, a quantum system is **perturbed**
3) Thus, any action performed introduces **noise**

QKD in a nutshell

1) "Encode" the key sequence in a stream of **qubits**
2) Estimate how much information **Eve** has
3) Establish a truly **random and secret** key
4) Safely perform **one-time pad**



No-cloning theorem

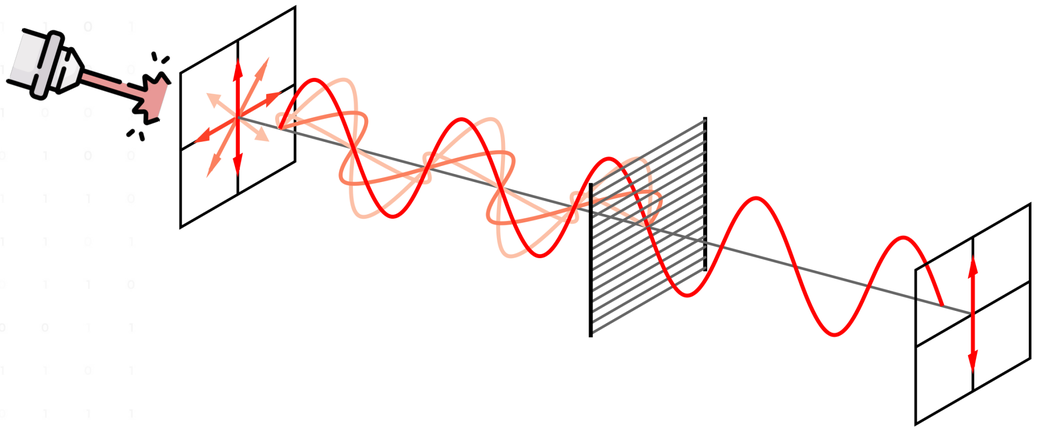
A quantum copy machine ***cannot*** exist!

Photons as Qubits

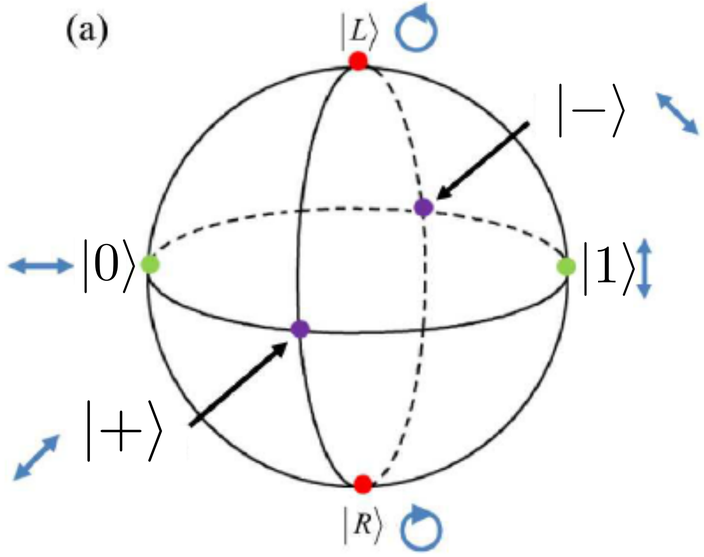
Any system with a **two-level** quantum description!

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

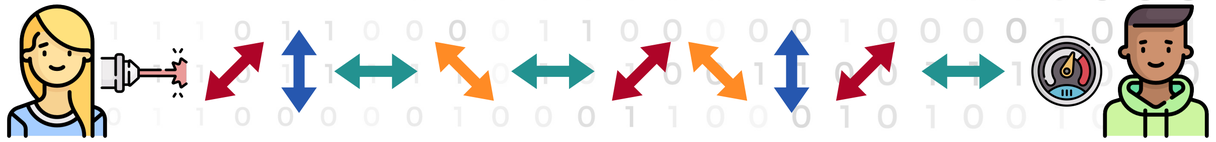
How it can be done? **Photons!**



Encode a qubit in their ***polarisation***



Bloch Sphere Representation



BB84 QKD protocol

Exchange of stream of “randomly” polarised single* photons **prepared** by Alice and **measured** by Bob.

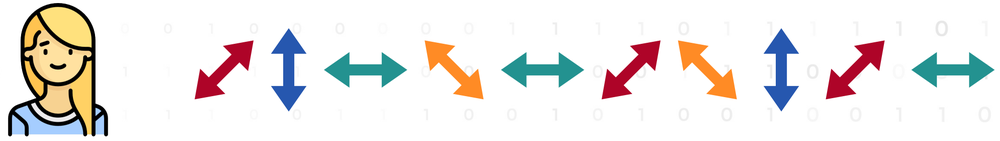
BB84 Protocol

Bennet, Brassard (1984)
Arxiv:2003.06557

Bit	Basis A	Basis B
0	$\|0\rangle$ ↔	$\|+\rangle$ ↗↘
1	$\|1\rangle$ ↕	$\|-\rangle$ ↘↗

Step 1: Pre-agreed encoding scheme

String	0	1	0	1	0	0	1	1	0	0
Basis	B	A	A	B	A	B	B	A	B	A

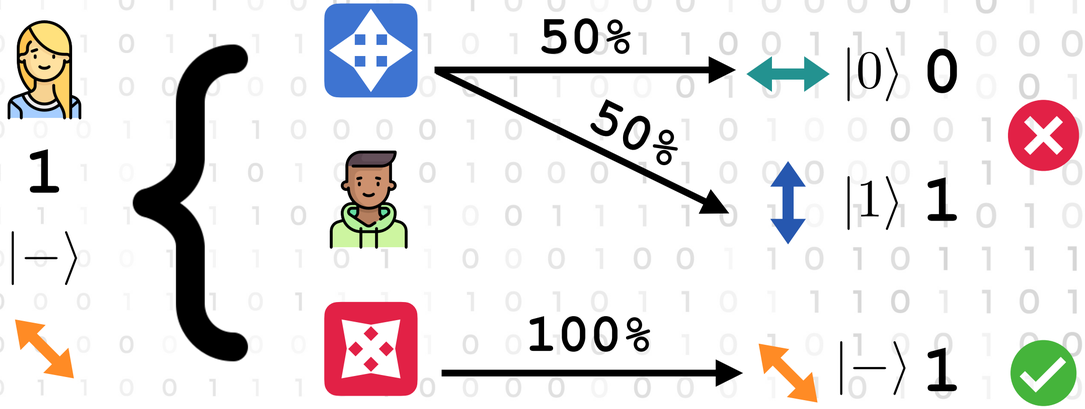


Step 2: Alice generates a random string of bits and a random choice of basis to encode her photons

Step 3: Bob measures the received photons in a random bases

Basis A **Basis B**

- The “right” basis recovers the **correct** bit
- The “wrong” basis yield a **random** result



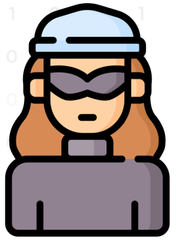
BB84 Protocol

Just a few more steps...

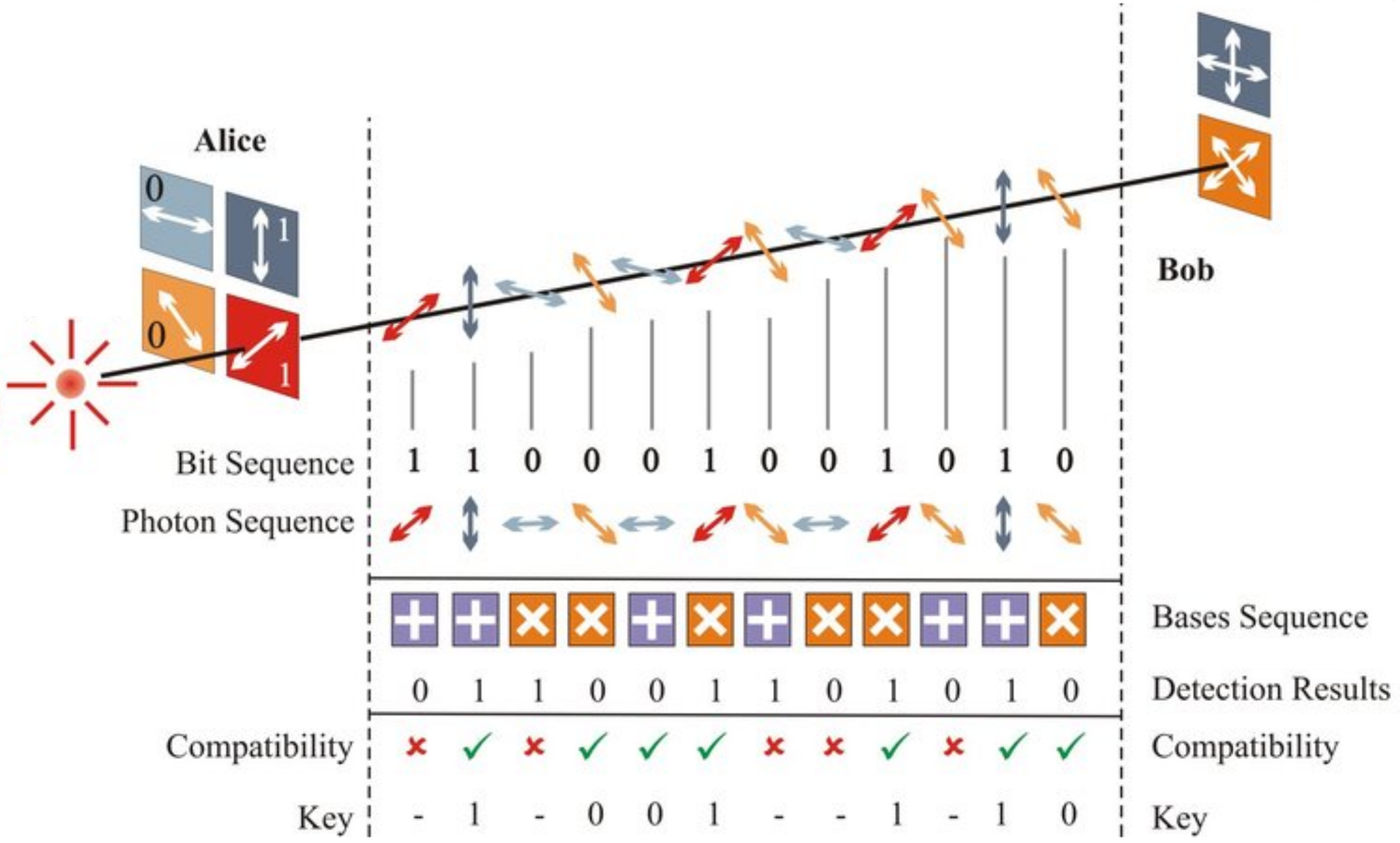
Alice and Bob **share** their bases choice over a *classical* channel

They **discard** the bits for which they used different bases

The remaining bits are the **common, random** and secure* key



***But wait! Where is Eve?**

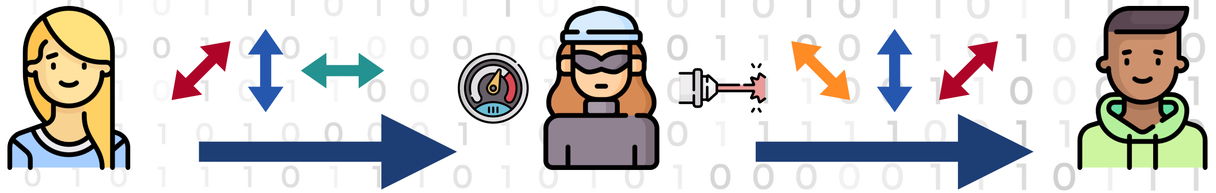


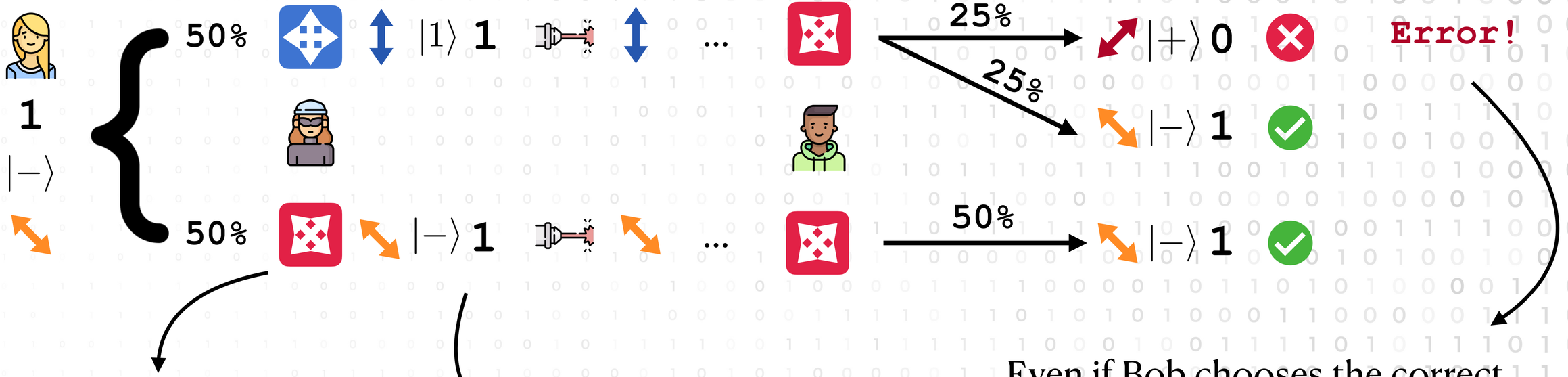
"Sifted Key"

Intercept-Resend

What if Eve **intercepts** the outgoing photons?

1) She must **measure,** thus *destroying* them
2) She must **resend** something to Bob





No **a-priori** information on what to measure

Resend a new photon according to her results

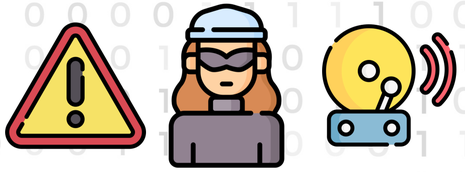
Even if Bob chooses the correct basis, there's a chance of recording an **error**

Quantum Bit Error Rate

10011100 00101101 11101001

10001101 00101011 10111000

$$\frac{\text{7 Errors}}{\text{24 Bits}} = 29\%$$



If any **discrepancy** in the sifted keys is present, then **Eve's** presence is **revealed**

How they can detect Eve's presence?

1) **Compare** (and discard) a subset of the key
2) Compute the **QBER,** i.e. the error ratio

$$QBER \equiv Q = \frac{\text{Number of errors}}{\text{Total Length}}$$

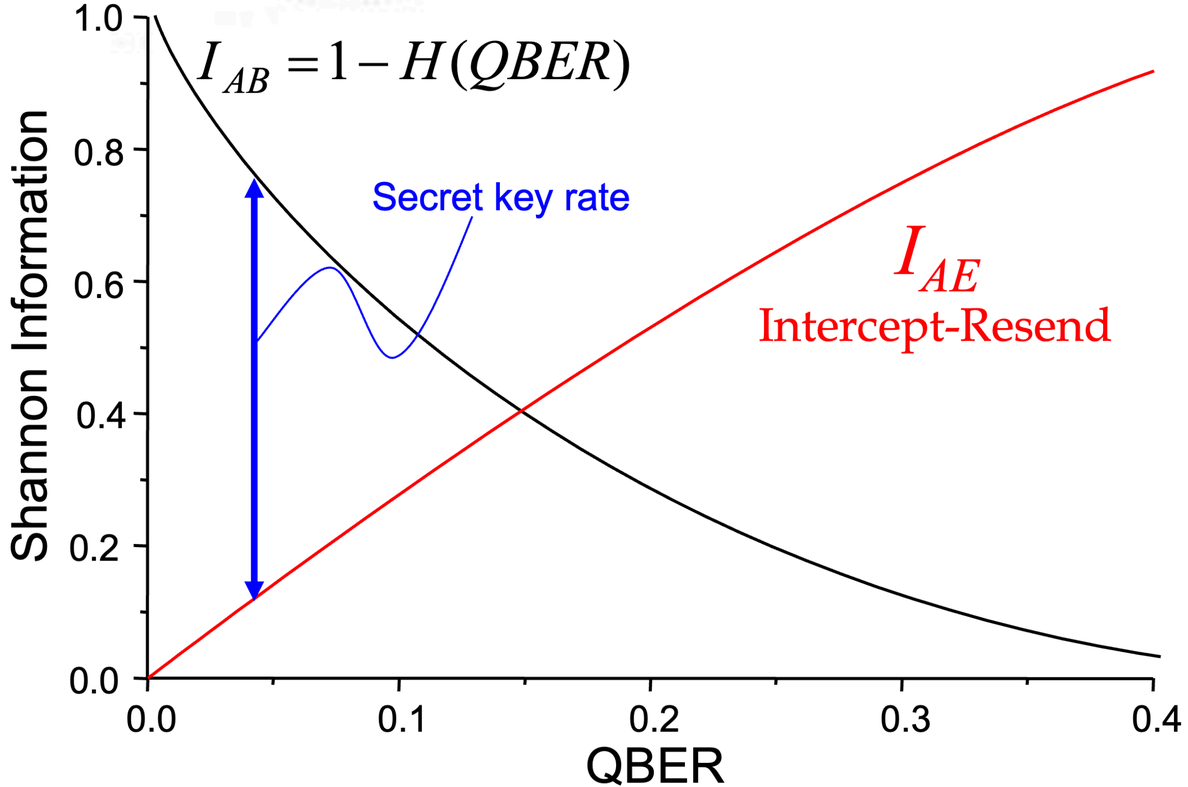
Making the Key secure

If Eve is detected, can we still extract a **secure** key?

$$I(A,B) \geq I(A,E)$$

Csiszar-Korner (1978)

Information is a function of the **QBER**



Mutual Information

Quantifies the "amount of information" obtained about one random variable by observing another random variable

$$I(A,B) = 0$$

Independent Variables

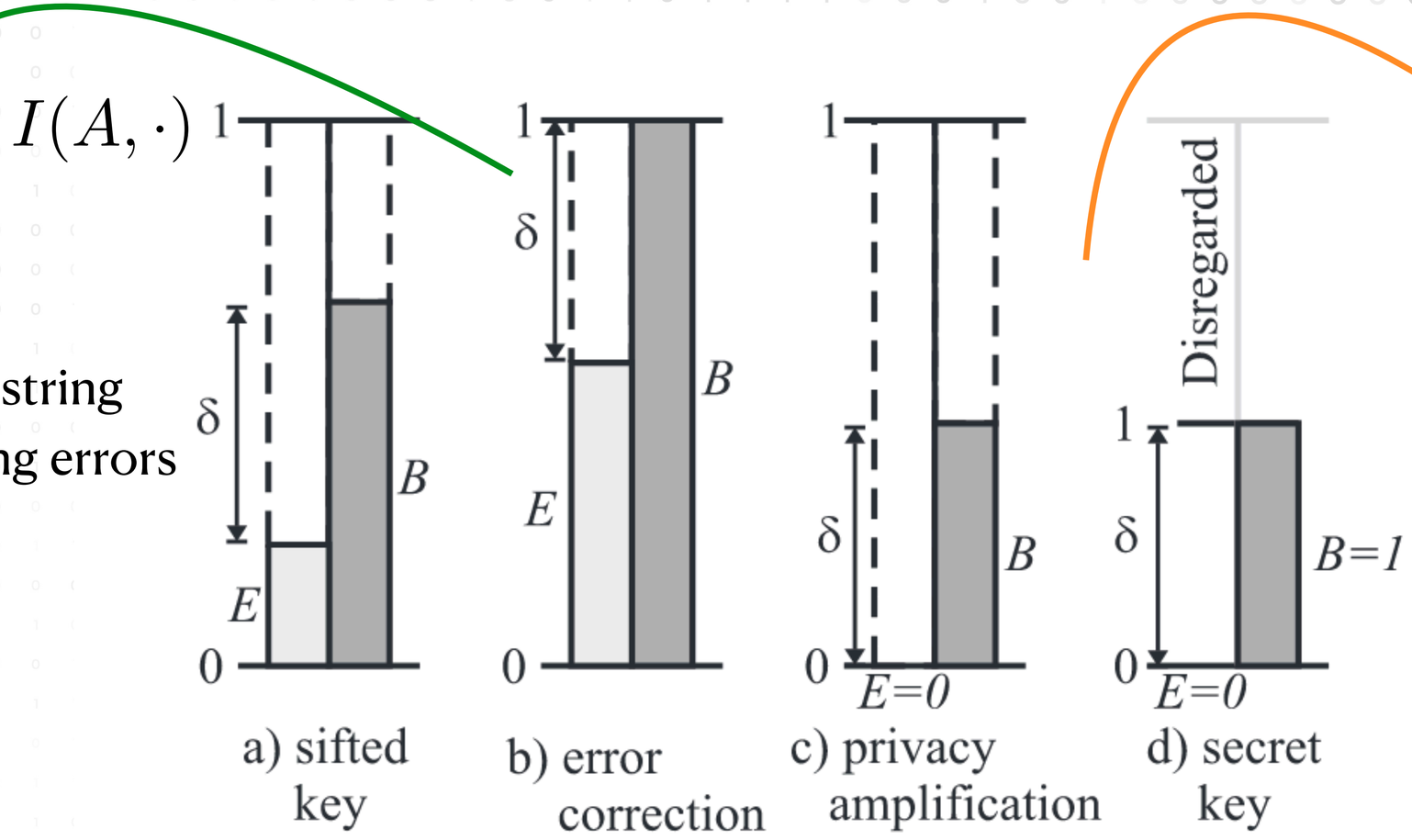
$$I(A,B) = 1$$

Fully Correlated

Making the Key secure

Employ well known classical algorithms: **error correction** and **privacy amplification**

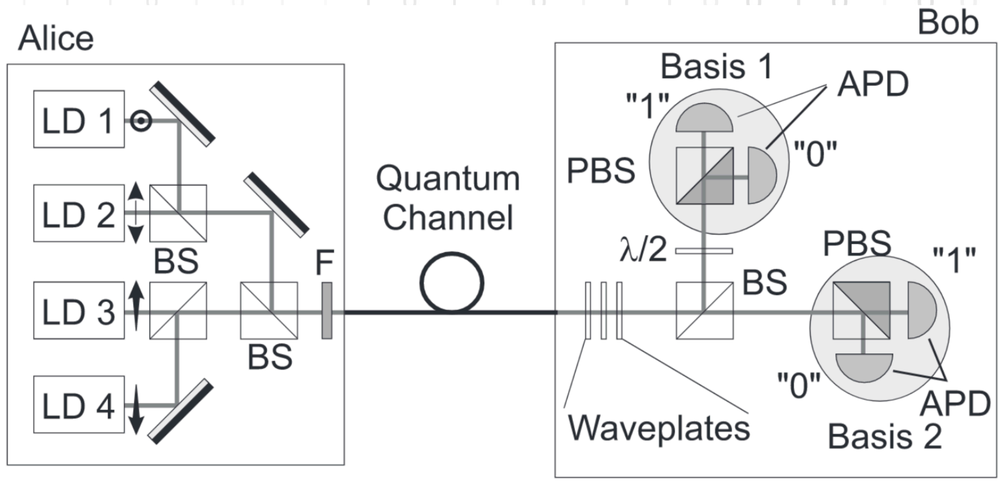
Cleans the bit string from the remaining errors



Destroy Eve's degree of information

$$\delta = I(A,B) - I(A,E)$$

A Typical QKD Setup



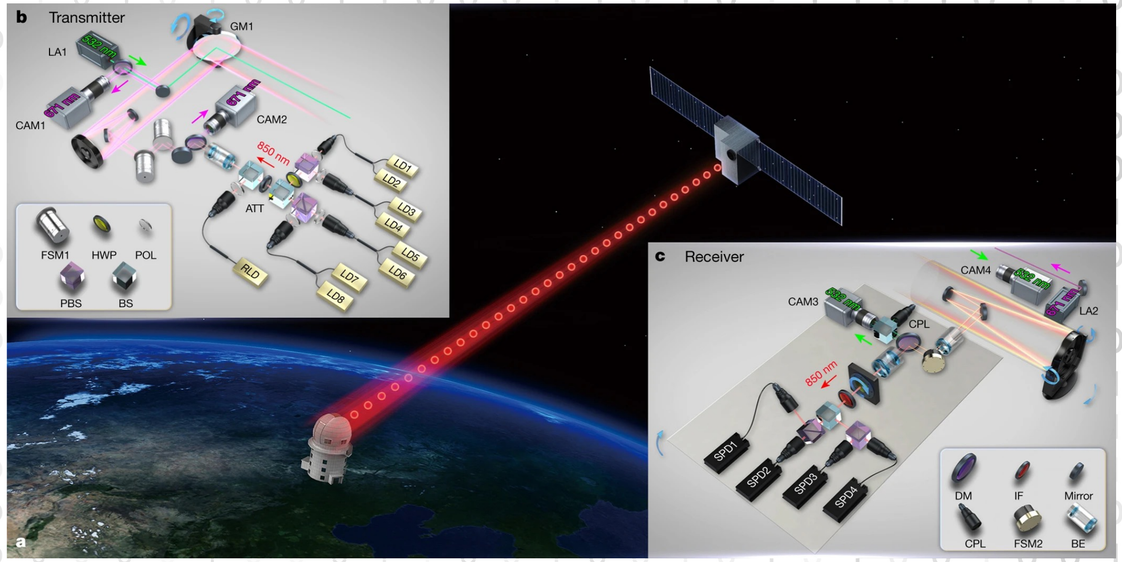
Faint laser pulses, generating basis states

Polarisation measurement stage

Fast synchronisation and **electronic** control needed

It's commercial...

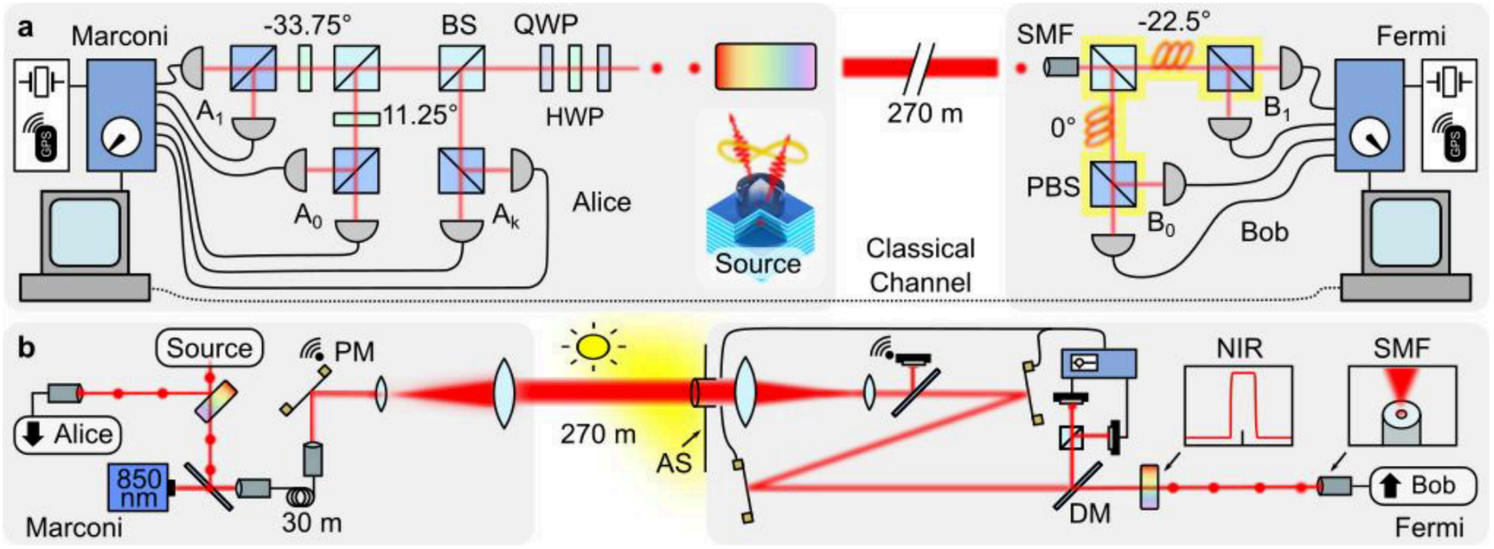
...and even through space!

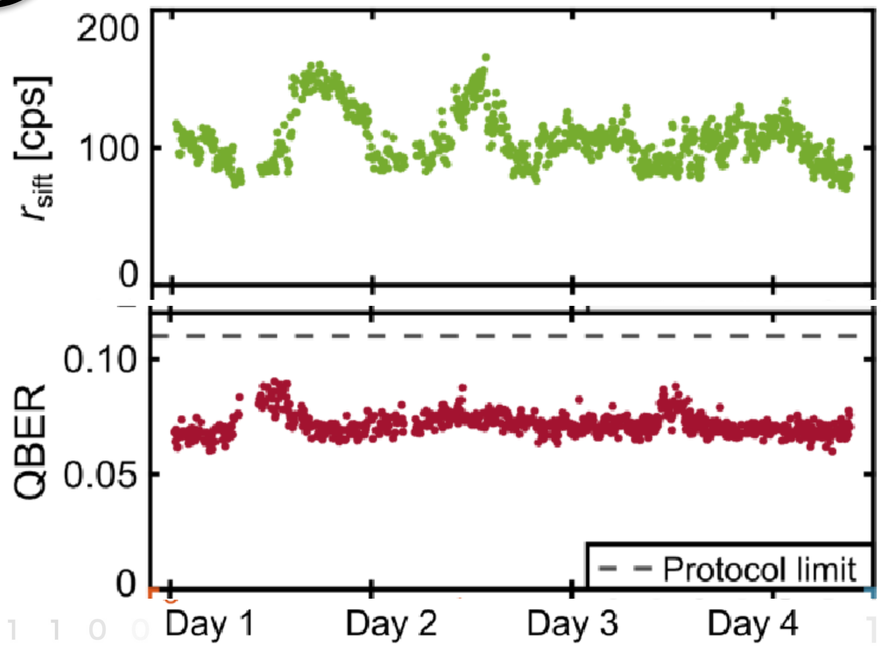


[Nature](#) **549**, 43–47 (2017)

And we did too!

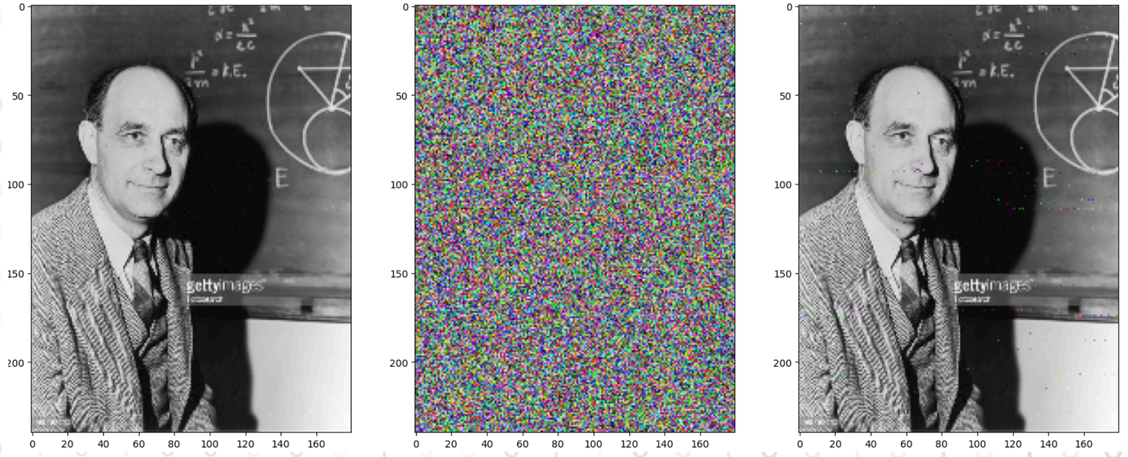
Arxiv:2206.15360





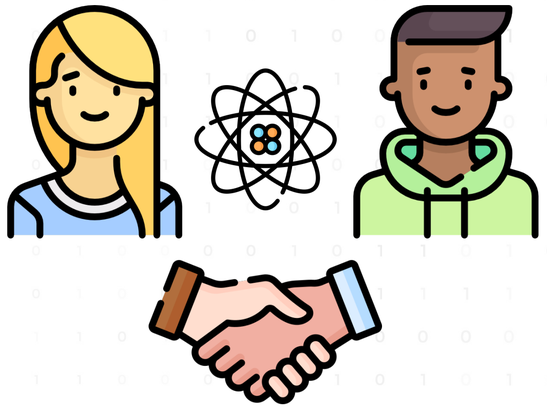
Main Points

- **Entanglement** based protocol
- Active **beam stabilisation**
- Time **synchronisation** with GPS



Message Encrypted Decrypted

Takeaways



1. Modern cryptography is **not** Quantum proof
2. **Quantum Mechanics** solves the *key distribution problem*
3. **QKD** protocols exist and are **practical**

Thank You!