

# Quantum Safe Security Process

**Bruno Sanglé-Ferrière**

*Chief Executive Officer, Carrousel Digital*

in **DigiGov Expo**

**DIGIGOVEXPO**

SPONSORED BY



Carrousel Digital

# quantum safe security process



Digigov 24 Excel London May 7<sup>th</sup> -8<sup>th</sup> 2024 [www.carrousel.digital](http://www.carrousel.digital) Bruno Sanglé-Ferrière, CEO  
patents US20230021900A1, US16793123 ,FR2208919, FR3092923B1



# What we do



IP Provider we design and license our IP to users and manufacturers

Quantum safe security : communication, e-signature and passive router

Other features :

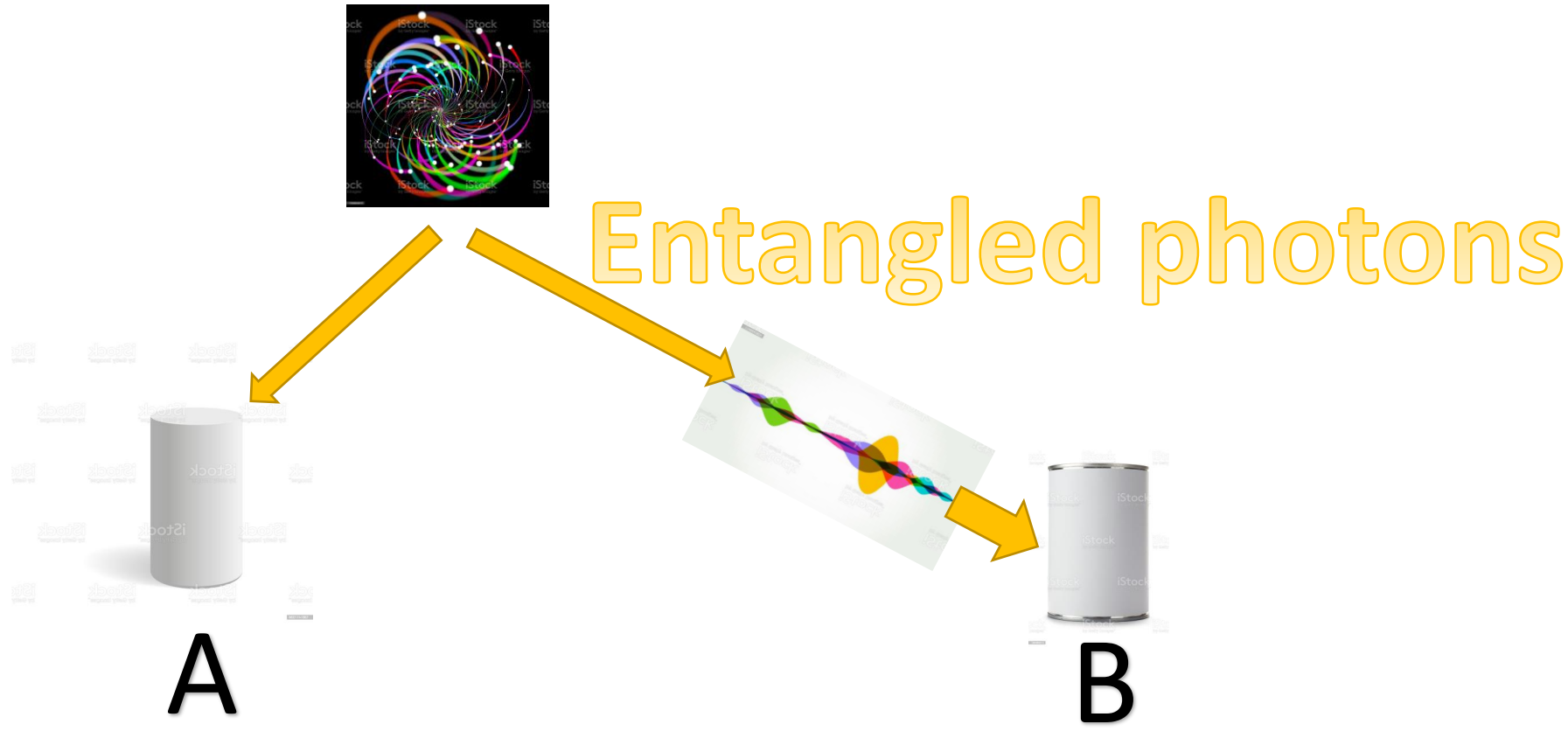
<p>➤ Indoor geo-localisation based on Long waves and medium frequencies</p> 	<p>➤ One time key distribution over the internet</p>
<p>➤ Memory protection upon firmware updates by deleting communication keys</p>	<p>➤ Long distance quantum teleportation</p>
<p>➤ Online/offline e-identity</p>	<p>➤ Online/offline cash medium</p> 

# Secure and fast data communication

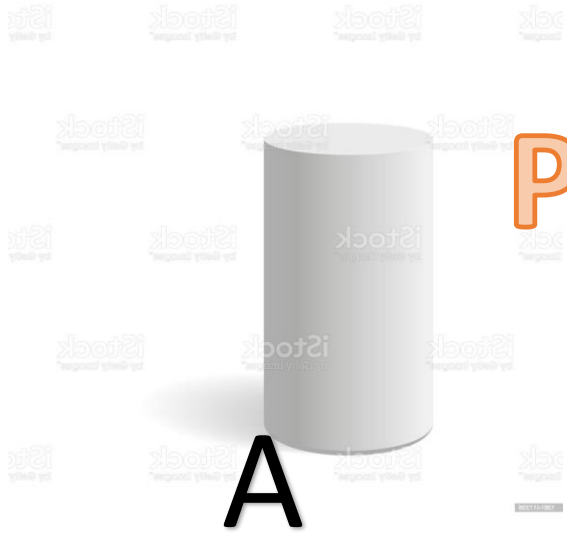


Entangled photon communication

# Sending entangled photons



# Coding the photons



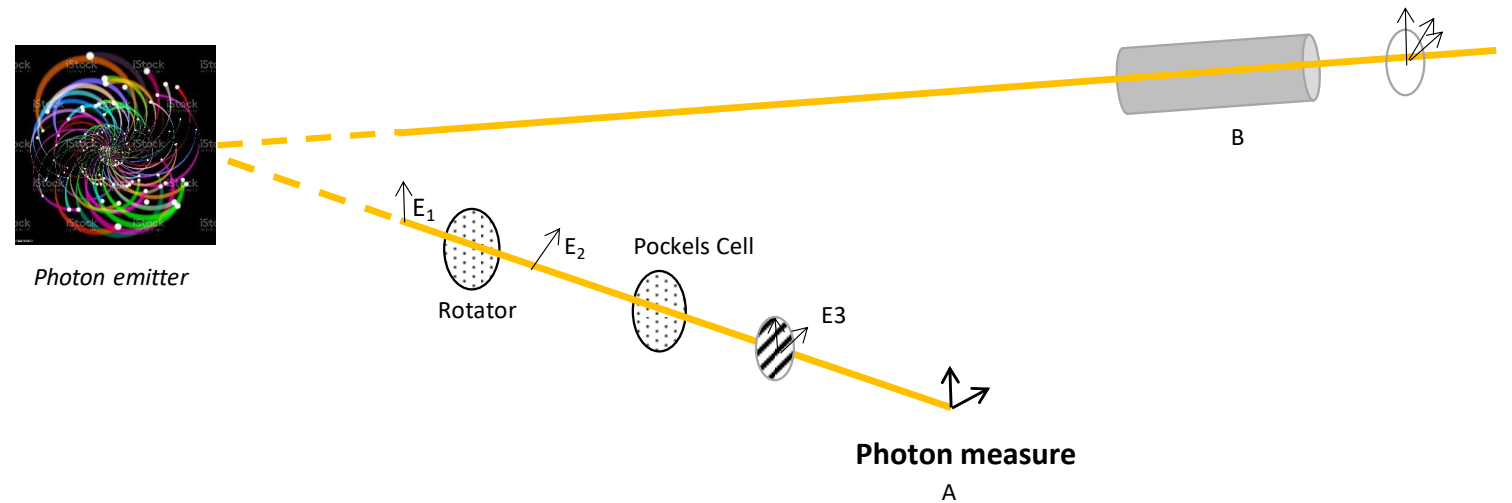
Polarisation angle  $\theta$  or  $\theta+90^\circ$

Polarisation elipcity  $\phi$



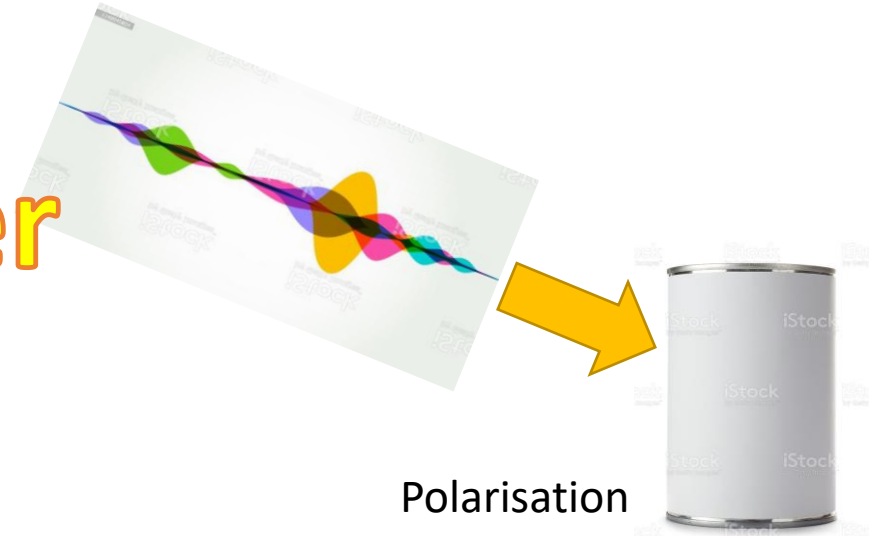
# Coding the photons

- Measuring the polarisation in either of two perpendicular directions
- After the photon polarisation has been modified



# Reading the code

amplifier



Polarisation  
angle and ellipticity reading

**B**





# Checking the message

- Photons traveling to A may be lost
- Photons arriving in B may be polarised in a way not related to the photon coding in A
- Statistically a lot more photons will arrive as coded in A though
- We set a number of identical received codes over a set number of successively received photons to detect a sent information



The system is **FAST**

Coding a photon in A immediately changes the polarisation of the photon traveling to B

the photons were entangled

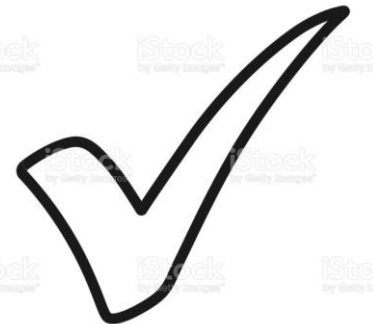
and already far apart



# Security check

Make sure photons arrive in B entangled to another photon arriving in A by :

- placing a polarisation filter at the data receiver to make sure their polarisation gets changed later by their encoding.
- Verify the matching of the exact polarisation of entangled photons arrived in A and B ; by exchanging a signed message with the arrival times and exact polarisations of the detected photons



# Security check for free-space transmission

- Capture or copy of some of the traveling photons traveling to B while not encoded will either
  - decrease the rates of photons arriving in B
  - or decrease the ratio of photons in B encoded
- These two events can be detected in B when checking the message



# Security check for optical fibres

Monitor the travel path between the photon emitter and the B receiver.

- by placing the photon emitter, the fibre linking it to the B receiver in the same box as the data receiver.
- As the travel paths quality of the line between the photon emitter and the data receiver could be enhanced in order to extract some of its photons, undetected threw the counting of arriving photons.

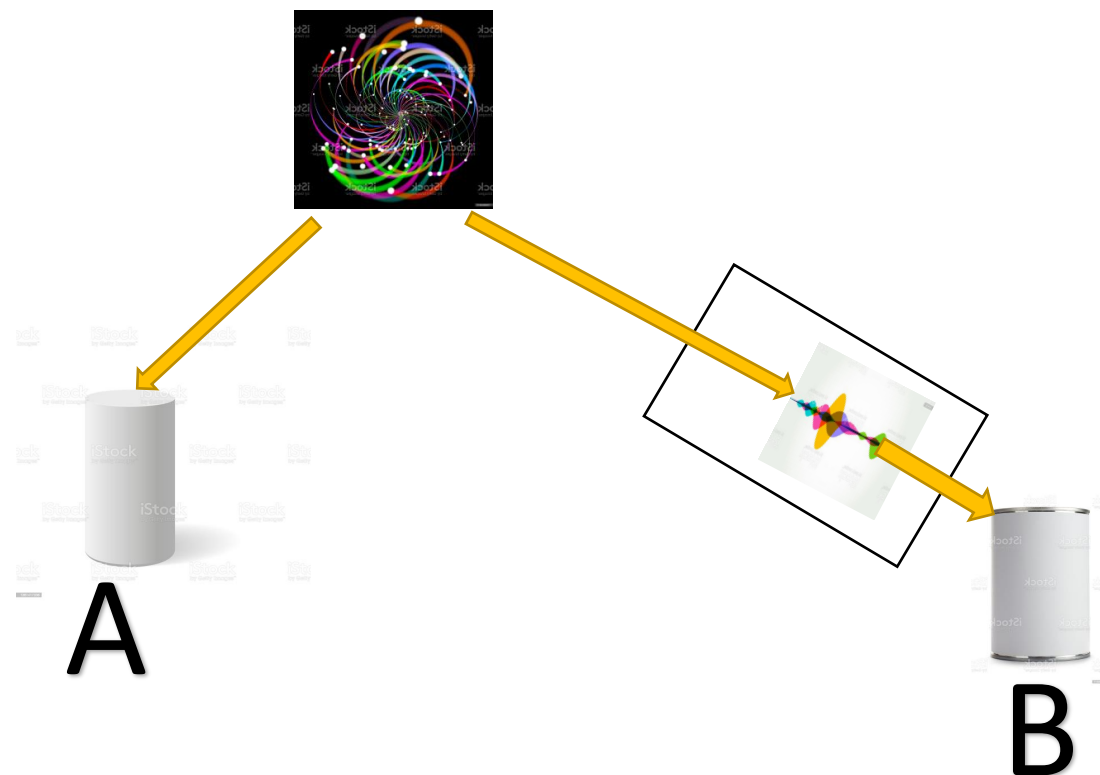
This limits secure entangled photon communication using optical fibres to a range of about 100km.



# Man in the middle

Where a 'spying' device sends to B specially crafted photons

- we install a **surveillance box** close to B
- photons arrive entangled in it
- If not they will be late
- Comparing the exact polarisation of the photons that reached both A and B will detect any unmatching of the exact polarisations.
- Can be done by exchanging a signed message of these exact polarisations and arrival times
- Preferably using a quantum safe signature like our patented random hash signature



# Physical link

Fiber optics

200km 90% loss



Free space

1000km

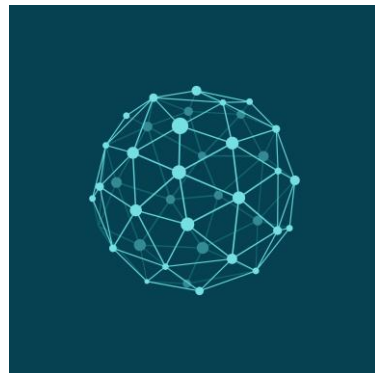
Satelite in the middle





# Application scenarios

Leverage on your optical fibre network



Build worldwide ground cover with 600 satellites at 500km altitude

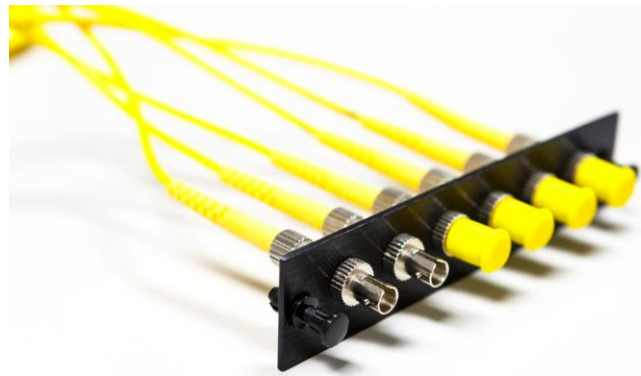
Link distant CPUs



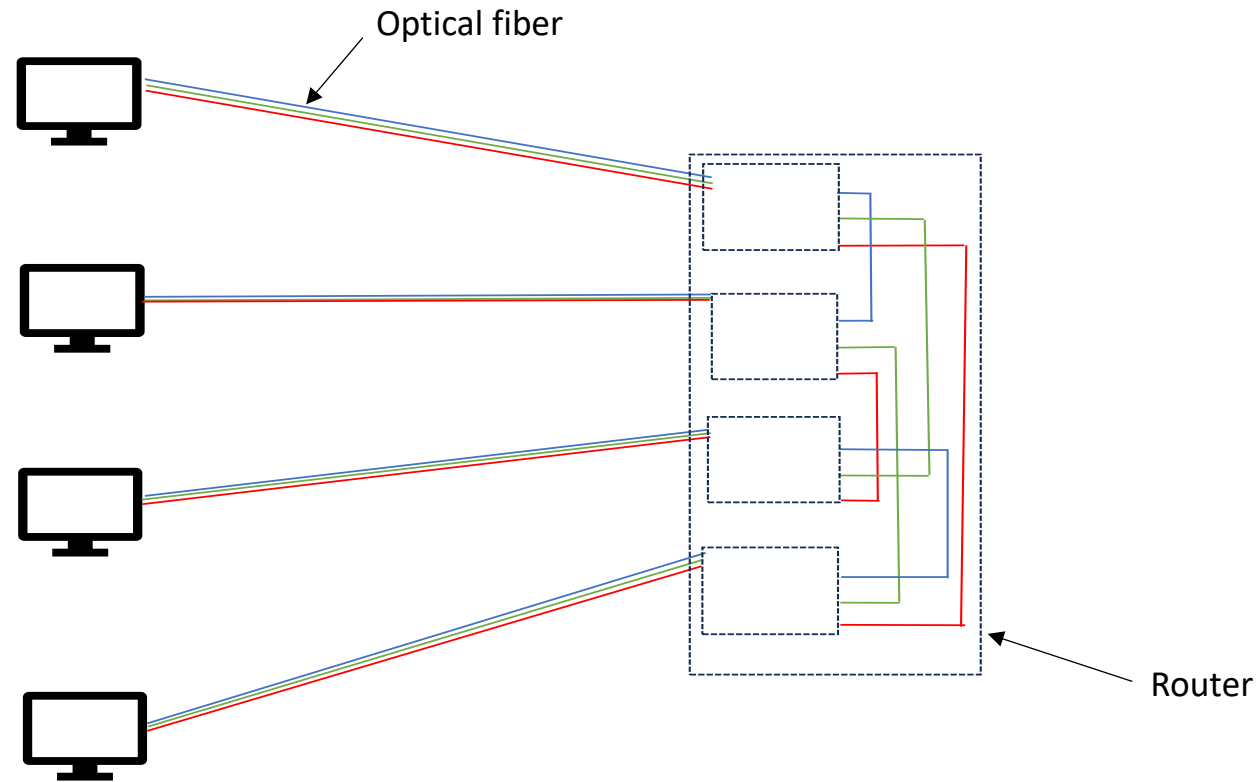


# Photonic Router

- One router
- Multiple quantum terminals
- Only one optical fiber between the router and each terminal



# Photonic Router



# Random Hash signatures

- Quantum Safe
- Simple processing required

# # # # #  
# # # # #  
# # # # #  
# # # # #  
# # # # #  
# # # # #



# Needs

- Hashing function such as SHA1 or SHA2
- Shared secret with between recipient and sender
- One Time Keys



# Process

1. Insert the secret in the document
2. Hash the resulting document
3. Encrypt the hash with a One Time Key (OTK)



# Proof the signature is secure

After the document has been sent, you may intercept :

- Clear text document
- The encrypted hash

No one can recompute the One Time Key as no one knows what the hash has been computed from.



# Please change the OTK each time

Please change the OTK otherwise you will have two equations if you intercept two documents and their signatures, enabling to find the two variables i.e. the Onetime key and the secret number.





*Entangled photon communication  
& Quantum safe signature*



Carrousel Digital Limited<sup>®</sup>

[www.carrouseldigital.com](http://www.carrouseldigital.com)