CESGA
GALICIA SUPERCOMPUTING CENTER

Nueva línea de comunicaciones cuánticas Santiago-Vigo

David Barral
Técnico coordinador de proyecto PCCC

Financiado por la Unión Europea
NextGenerationEU

AXENCIA GALEGA DE INNOVACIÓN

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

Plan de Recuperación, Transformación y Resiliencia

Cryptography

Confidential communication through cipher techniques

Financiado por la Unión Europea
NextGenerationEU

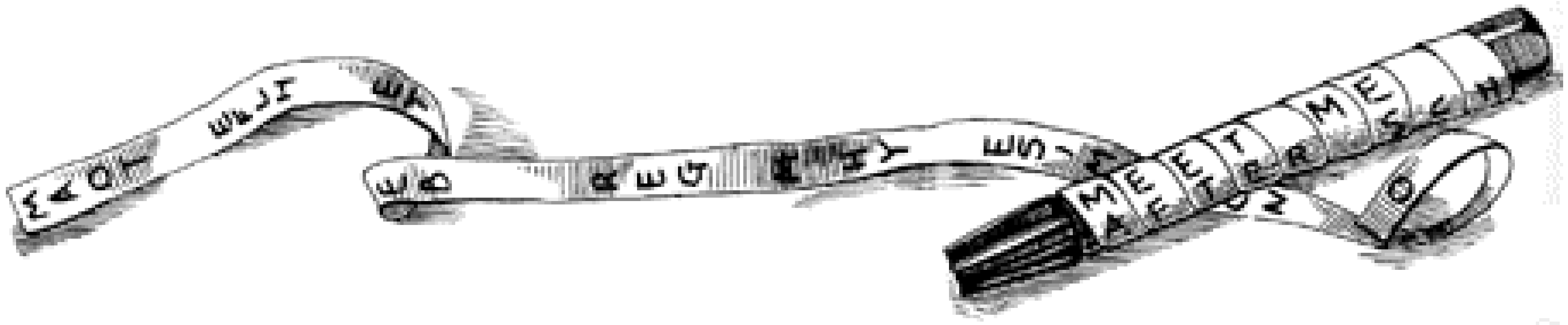
AXENCIA GALEGA DE INNOVACIÓN

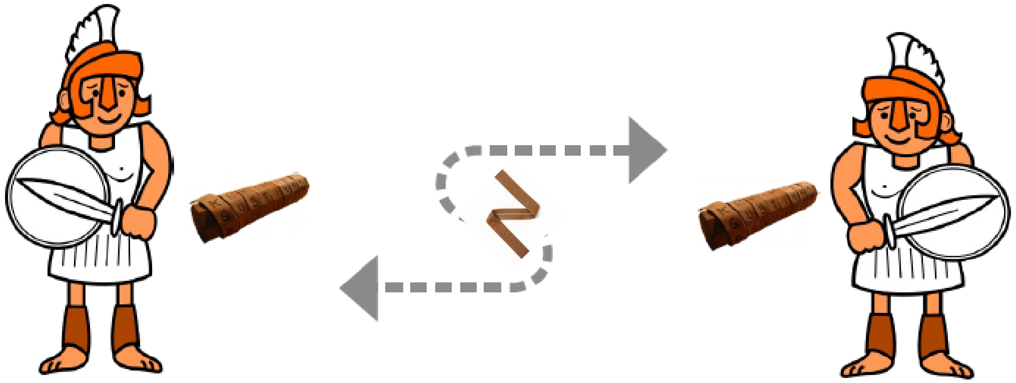
GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA E INNOVACIÓN

Plan de Recuperación, Transformación y Resiliencia

Scytale

(7th century B.C.)





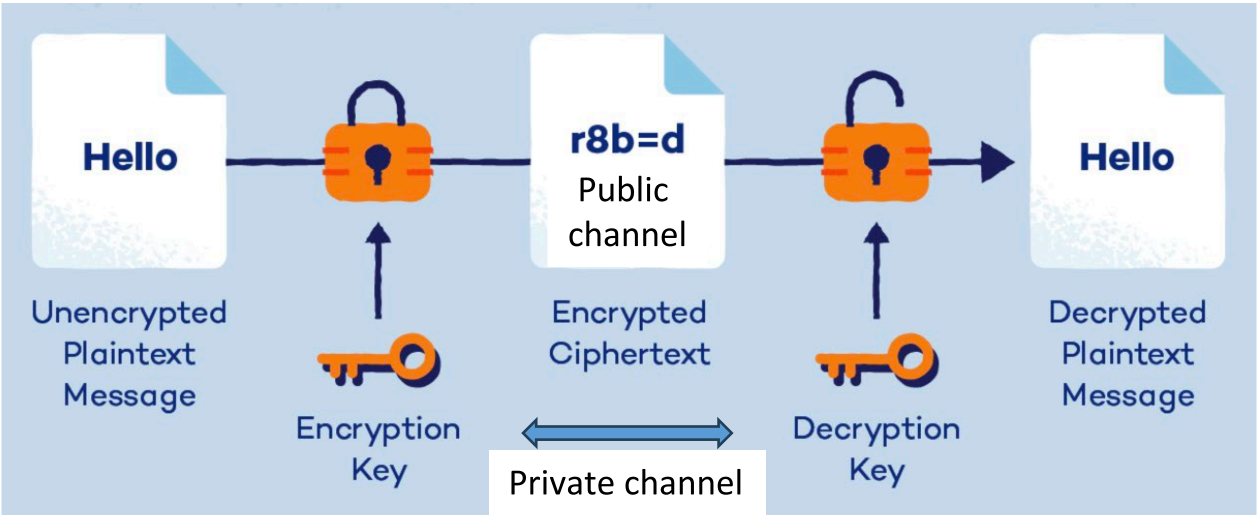
Financiado por
la Unión Europea
NextGenerationEU

AXENCIA
GALEGA DE
INNOVACIÓN

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

Plan de
Recuperación,
Transformación
y Resiliencia

Cryptography

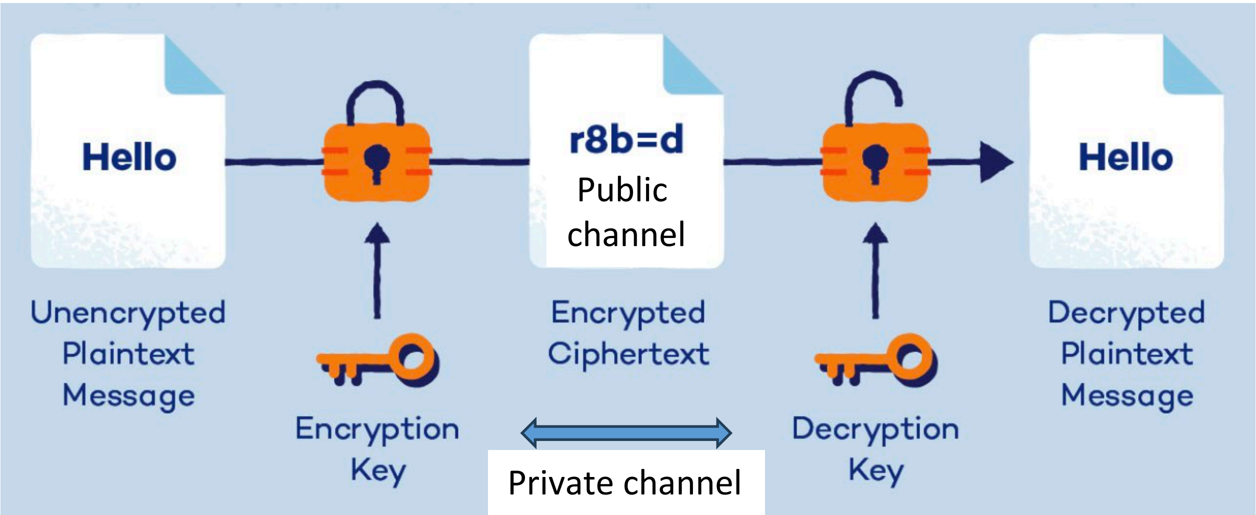


Financiado por la Unión Europea NextGenerationEU
AXENCIA GALEGA DE INNOVACIÓN
GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA E INNOVACIÓN
Plan de Recuperación, Transformación y Resiliencia

Cryptography

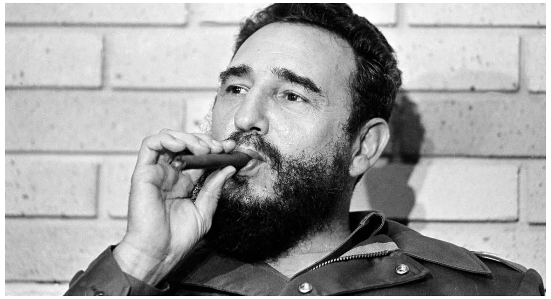
One time pad

(20th century)



Public channel

Private channel

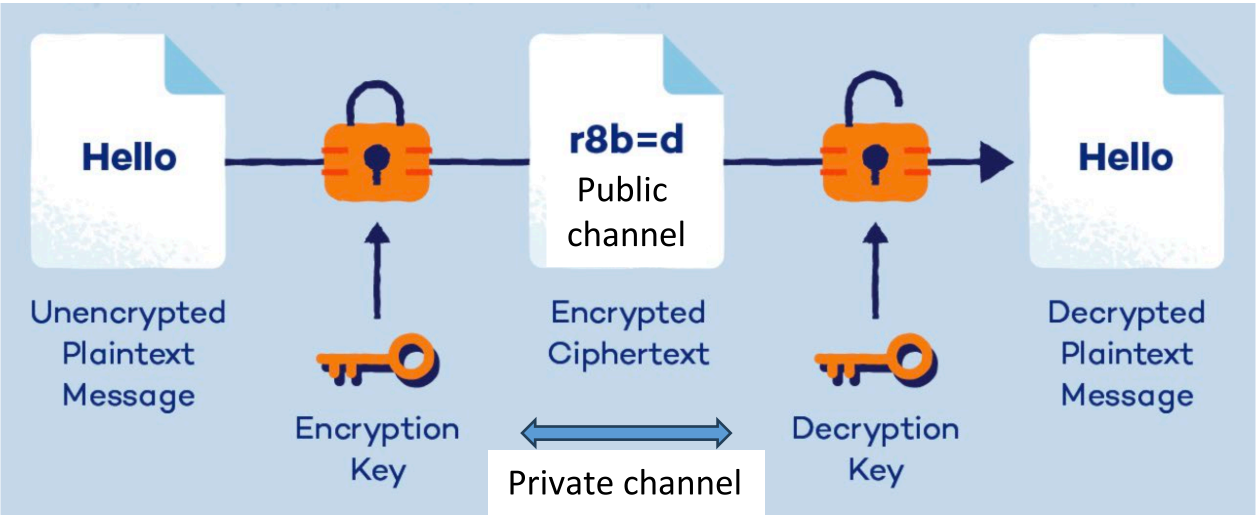


Financiado por la Unión Europea NextGenerationEU
AXENCIA GALEGA DE INNOVACIÓN
GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA E INNOVACIÓN
Plan de Recuperación, Transformación y Resiliencia

Cryptography

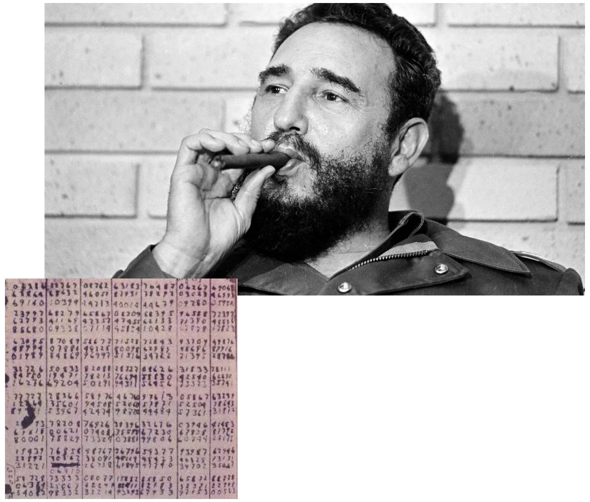
One time pad

(20th century)



Public channel

Private channel

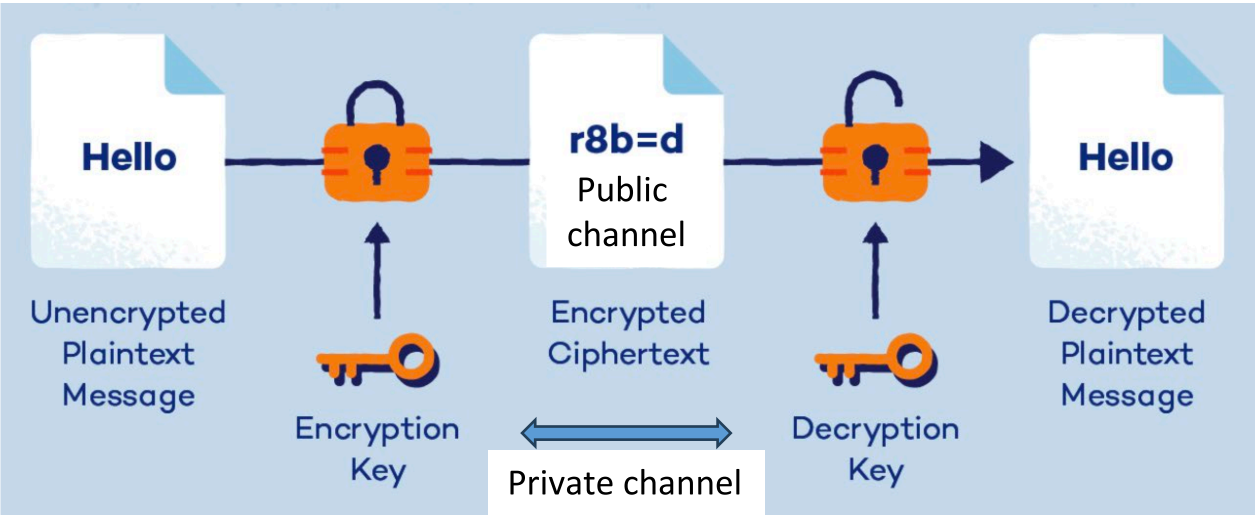


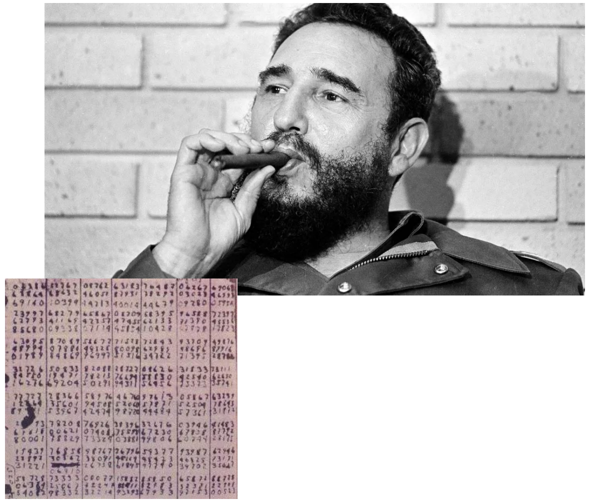
Financiado por la Unión Europea
NextGenerationEU
AXENCIA GALEGA DE INNOVACIÓN
GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN
Plan de Recuperación, Transformación y Resiliencia

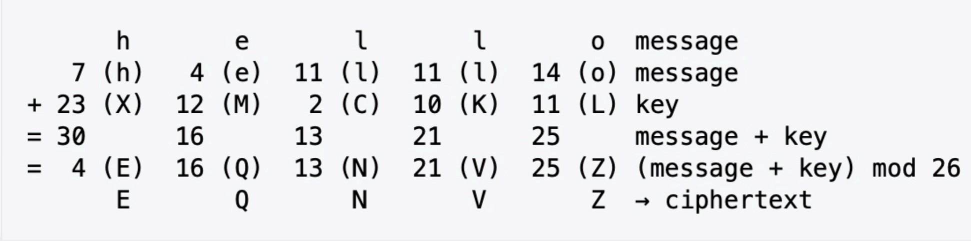
Cryptography

One time pad

(20th century)







```
       h        e        l        l        o  message
    7 (h)    4 (e)   11 (l)   11 (l)   14 (o)  message
+ 23 (X)   12 (M)    2 (C)   10 (K)   11 (L)  key
= 30       16       13       21       25      message + key
=  4 (E)   16 (Q)   13 (N)   21 (V)   25 (Z)  (message + key) mod 26
       E        Q        N        V        Z  → ciphertext
```

Financiado por
la Unión Europea
NextGenerationEU

AXENCIA
GALEGA DE
INNOVACIÓN

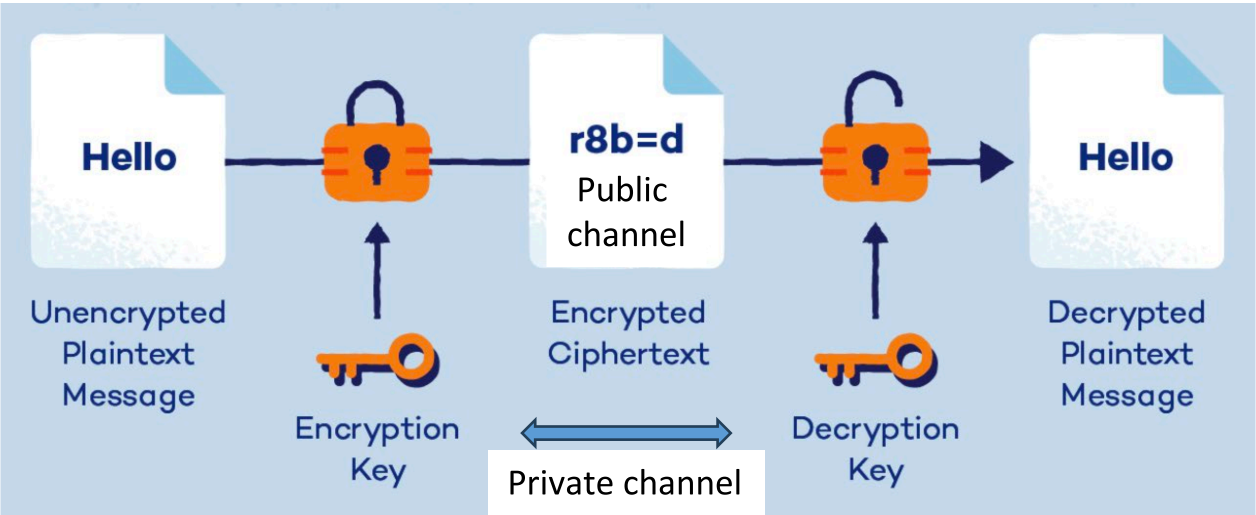
GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

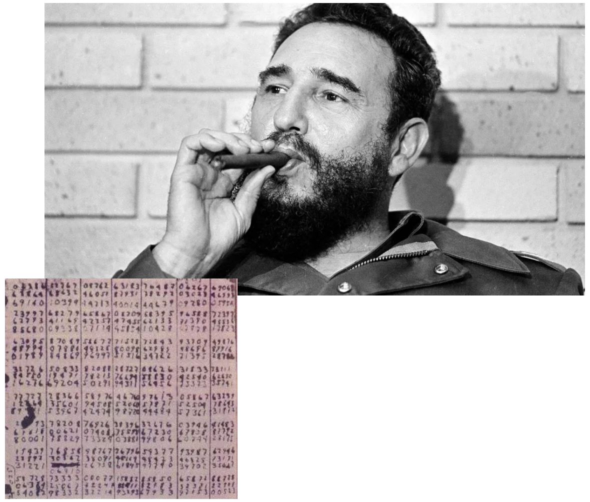
Plan de
Recuperación,
Transformación
y Resiliencia

Cryptography

One time pad

(20th century)





```
     h       e       l       l       o  message
   7 (h)   4 (e)  11 (l)  11 (l)  14 (o) message
+ 23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= 30      16      13      21      25     message + key
=  4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) (message + key) mod 26
     E       Q       N       V       Z  → ciphertext
```

```
       E       Q       N       V       Z  ciphertext
    4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) ciphertext
−  23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= −19       4      11      11      14     ciphertext − key
=   7 (h)   4 (e)  11 (l)  11 (l)  14 (o) ciphertext − key (mod 26)
       h       e       l       l       o  → message
```

Financiado por la Unión Europea
NextGenerationEU

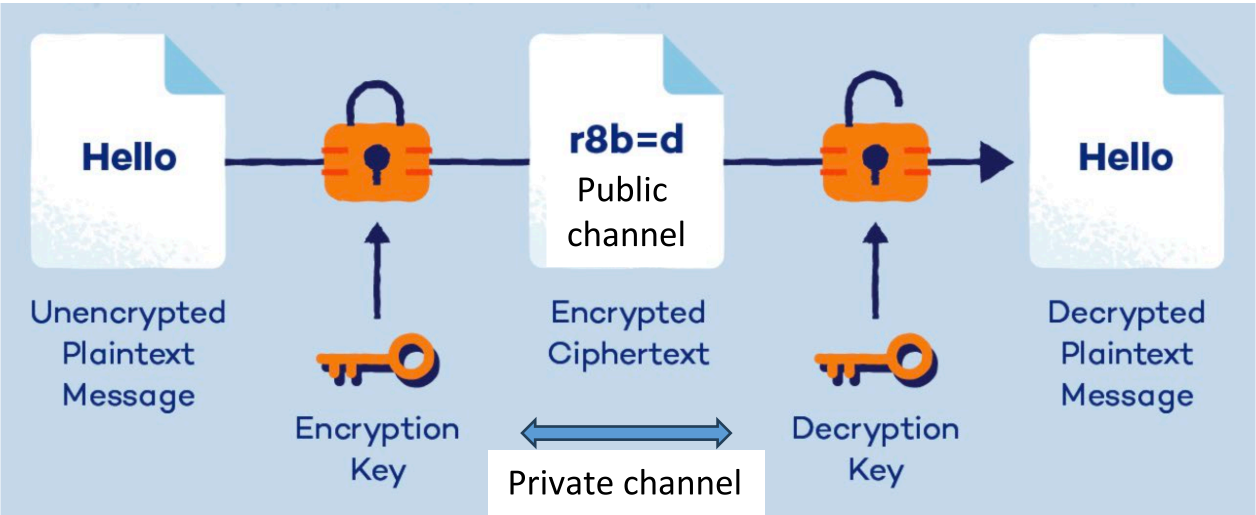
AXENCIA GALEGA DE INNOVACIÓN

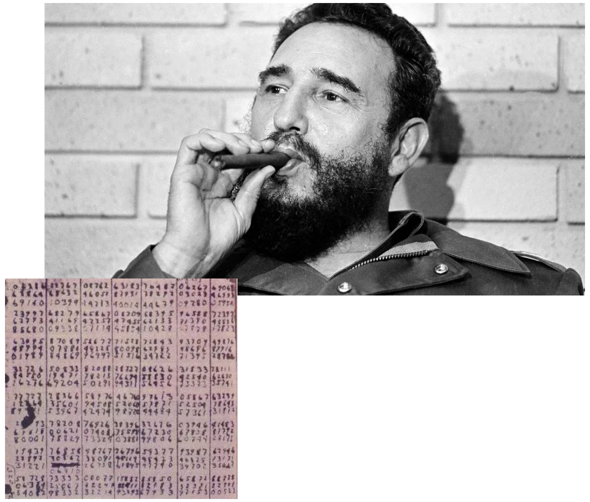
GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

Plan de Recuperación, Transformación y Resiliencia

One time pad

(20th century)





```
     h       e       l       l       o   message
   7 (h)   4 (e)  11 (l)  11 (l)  14 (o) message
+ 23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= 30      16      13      21      25     message + key
=  4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) (message + key) mod 26
     E       Q       N       V       Z   → ciphertext
```

```
      E       Q       N       V       Z   ciphertext
    4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) ciphertext
−  23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= −19       4      11      11      14     ciphertext − key
=   7 (h)   4 (e)  11 (l)  11 (l)  14 (o) ciphertext − key (mod 26)
      h       e       l       l       o   → message
```

Weakness: key transmission

Financiado por la Unión Europea NextGenerationEU

AXENCIA GALEGA DE INNOVACIÓN

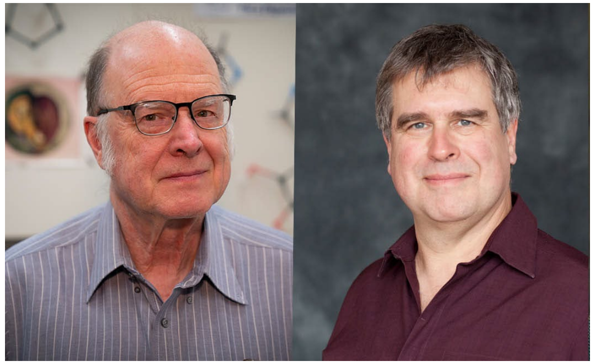
GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA E INNOVACIÓN

Plan de Recuperación, Transformación y Resiliencia

Quantum key distribution (QKD)

Secure key transmission (guaranteed by the laws of nature)

Proposed by Ch. Bennett and G. Brassard in 1984



Two quantum-mechanical ingredients:

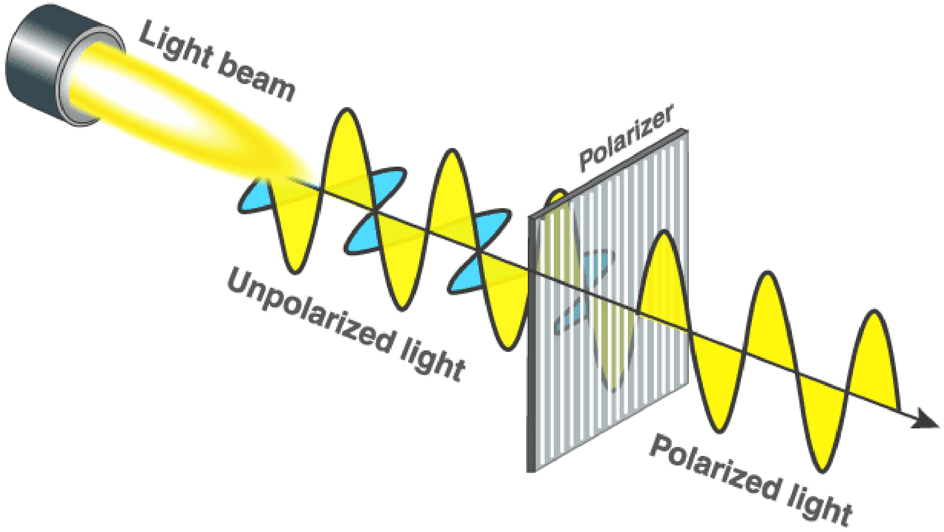
- Quantum uncertainty
- No-cloning theorem

Financiado por la Unión Europea NextGenerationEU
AXENCIA GALEGA DE INNOVACIÓN
GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA E INNOVACIÓN
Plan de Recuperación, Transformación y Resiliencia

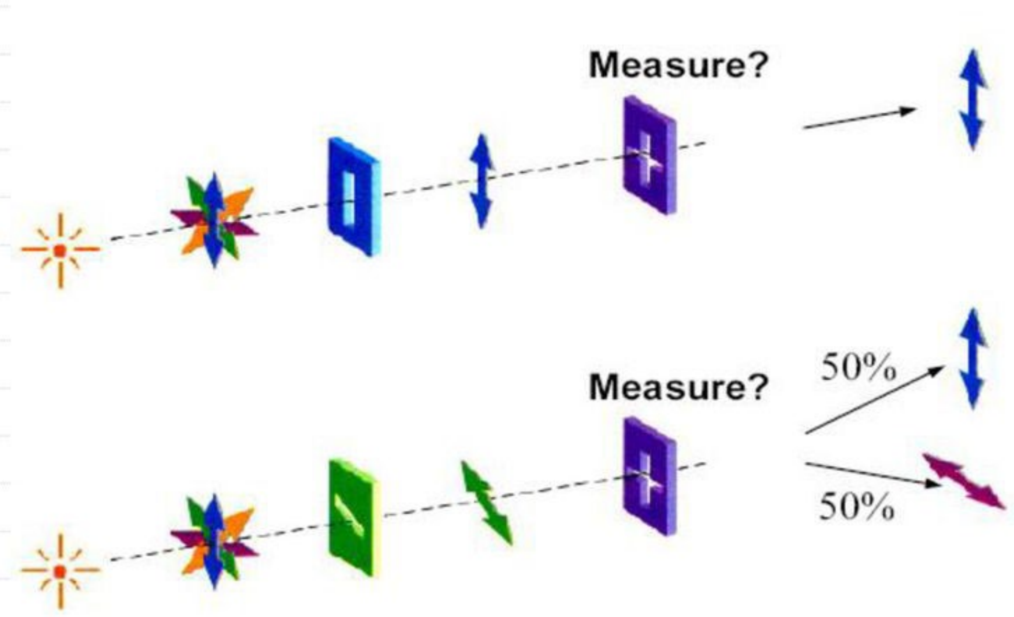
Quantum key distribution (QKD)

A photon is a wave and a particle

Wave: polarization

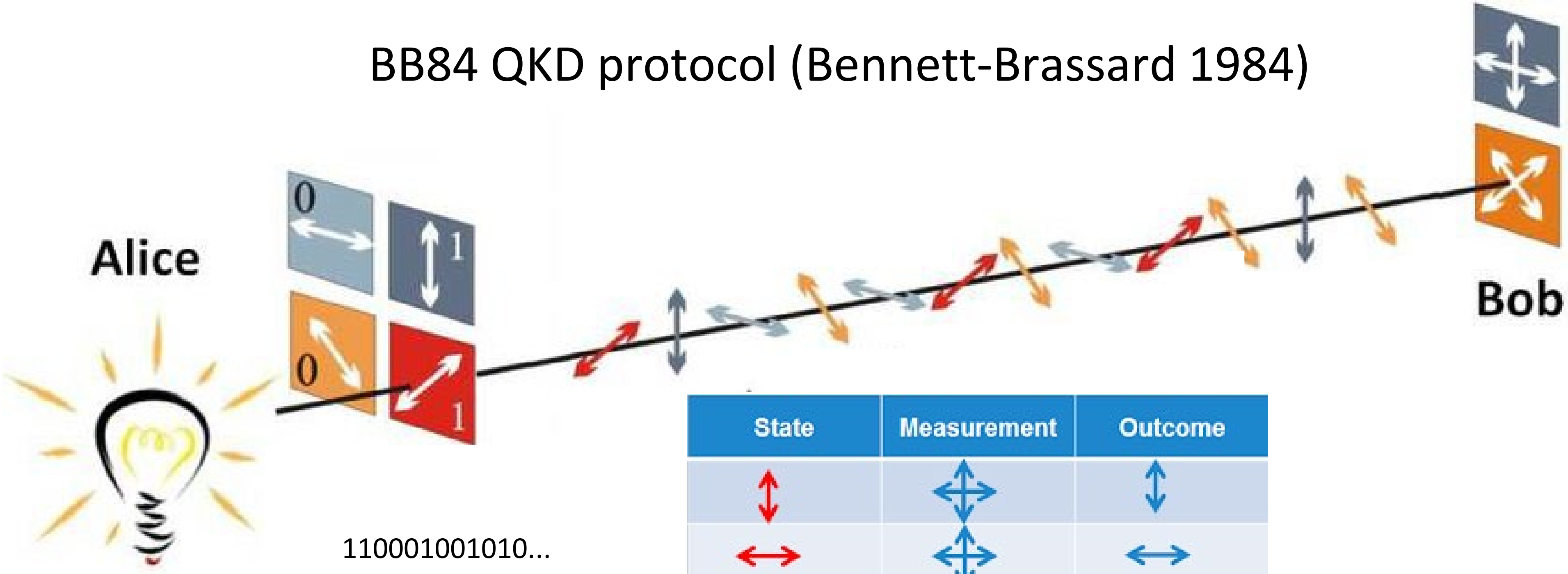


Particle: one "path" or "the other"



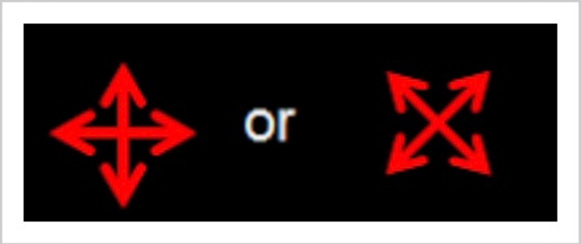
Quantum key distribution (QKD)

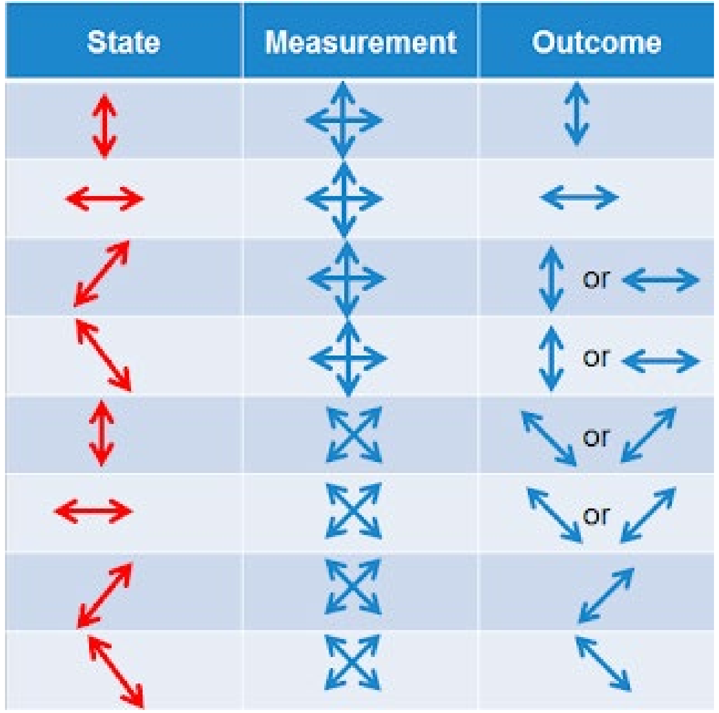
BB84 QKD protocol (Bennett-Brassard 1984)



110001001010...

1. Alice chooses a random sequence of bits and encodes each one using either:

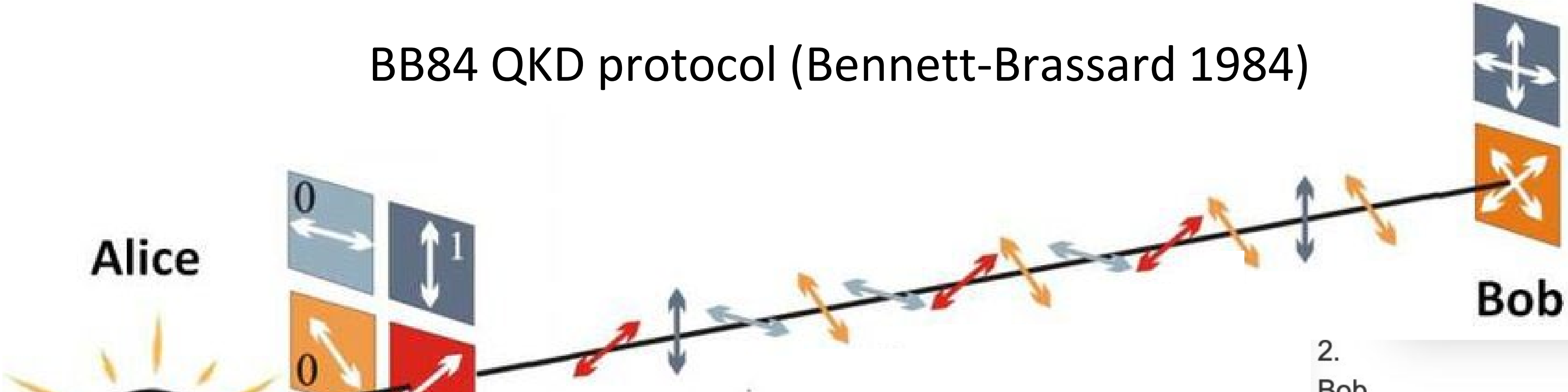




State	Measurement	Outcome
↕	✛	↕
↔	✛	↔
⤢	✛	↕ or ↔
⤡	✛	↕ or ↔
↕	✕	⤡ or ⤢
↔	✕	⤡ or ⤢
⤢	✕	⤢
⤡	✕	⤡

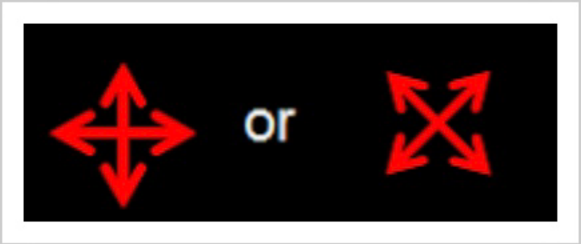
Quantum key distribution (QKD)

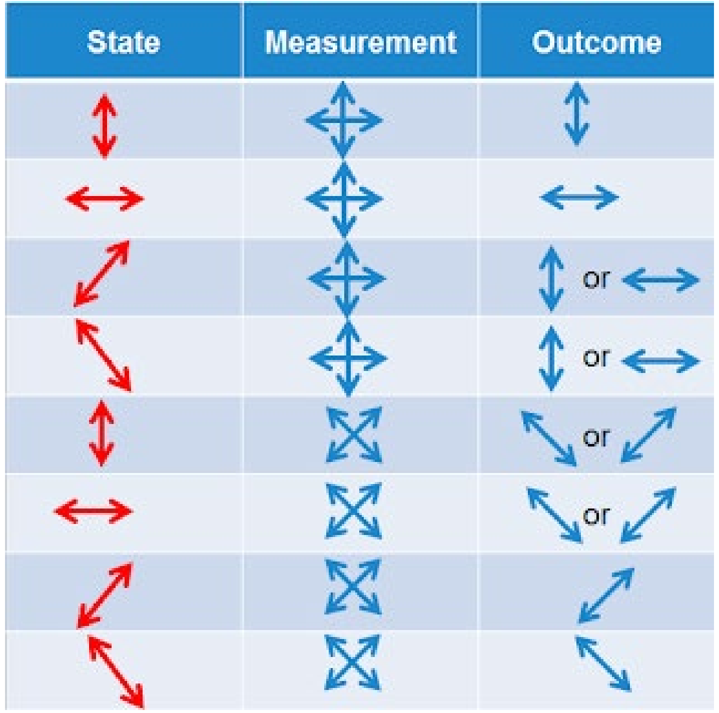
BB84 QKD protocol (Bennett-Brassard 1984)



110001001010...

1. Alice chooses a random sequence of bits and encodes each one using either:



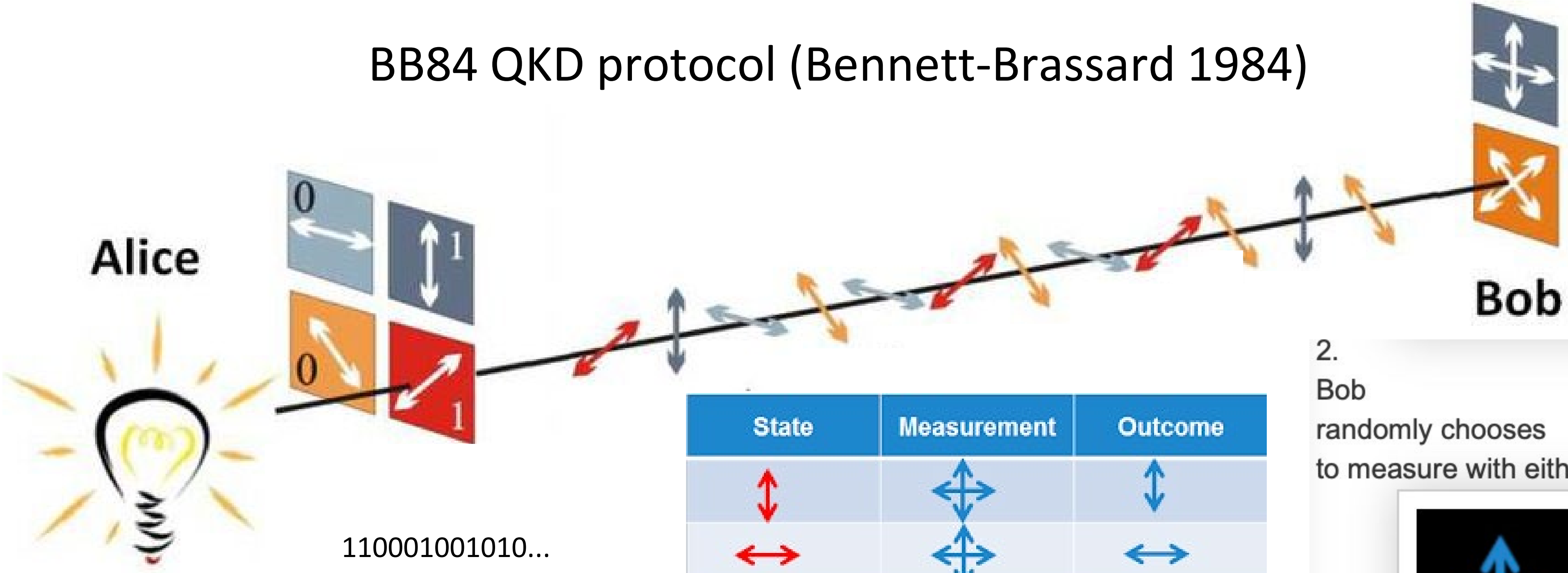


State	Measurement	Outcome
↕	✥	↕
↔	✥	↔
⤢	✥	↕ or ↔
⤡	✥	↕ or ↔
↕	✕	⤡ or ⤢
↔	✕	⤡ or ⤢
⤢	✕	⤢
⤡	✕	⤡

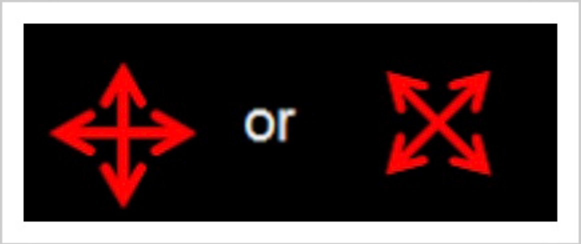
2. Bob randomly chooses to measure with either:

Quantum key distribution (QKD)

BB84 QKD protocol (Bennett-Brassard 1984)

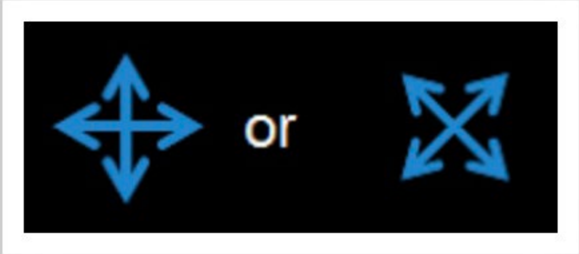


1. Alice chooses a random sequence of bits and encodes each one using either:



State	Measurement	Outcome
↕	✥	↕
↔	✥	↔
⤢	✥	↕ or ↔
⤡	✥	↕ or ↔
↕	⤧	⤡ or ⤢
↔	⤧	⤡ or ⤢
⤢	⤧	⤢
⤡	⤧	⤡

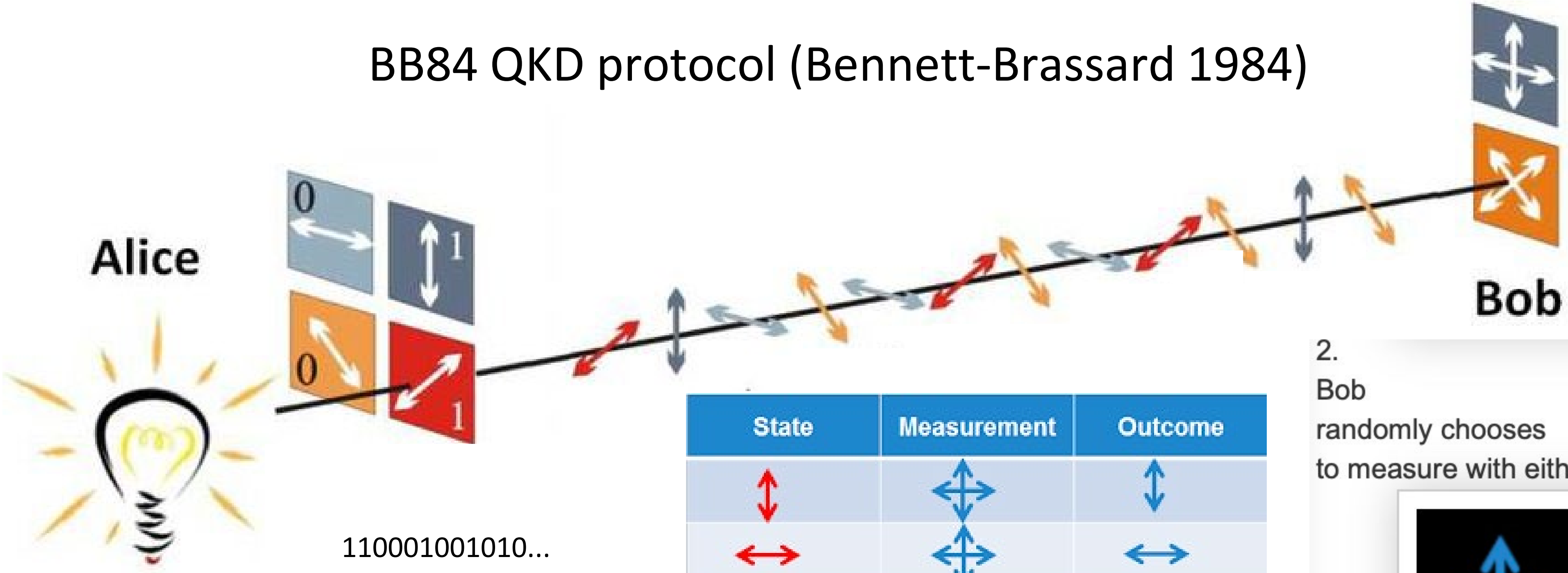
2.
Bob
randomly chooses
to measure with either:



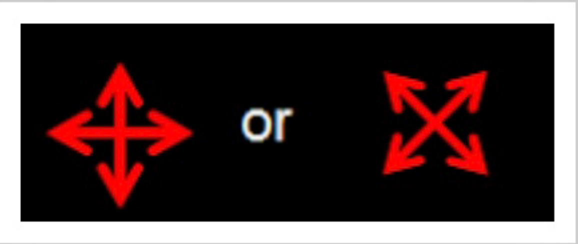
3.They publically reveal their choice of axes and discard pairs that don’t match.

Quantum key distribution (QKD)

BB84 QKD protocol (Bennett-Brassard 1984)

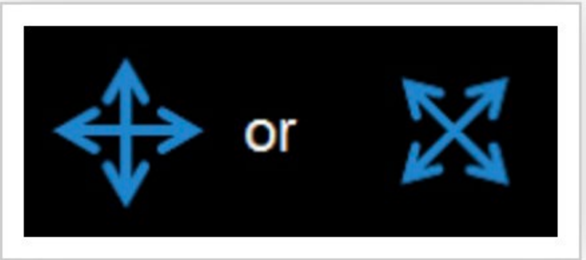


1. Alice chooses a random sequence of bits and encodes each one using either:



State	Measurement	Outcome
↕	✛	↕
↔	✛	↔
⤢	✛	↕ or ↔
⤡	✛	↕ or ↔
↕	✕	⤡ or ⤢
↔	✕	⤡ or ⤢
⤢	✕	⤢
⤡	✕	⤡

2. Bob randomly chooses to measure with either:

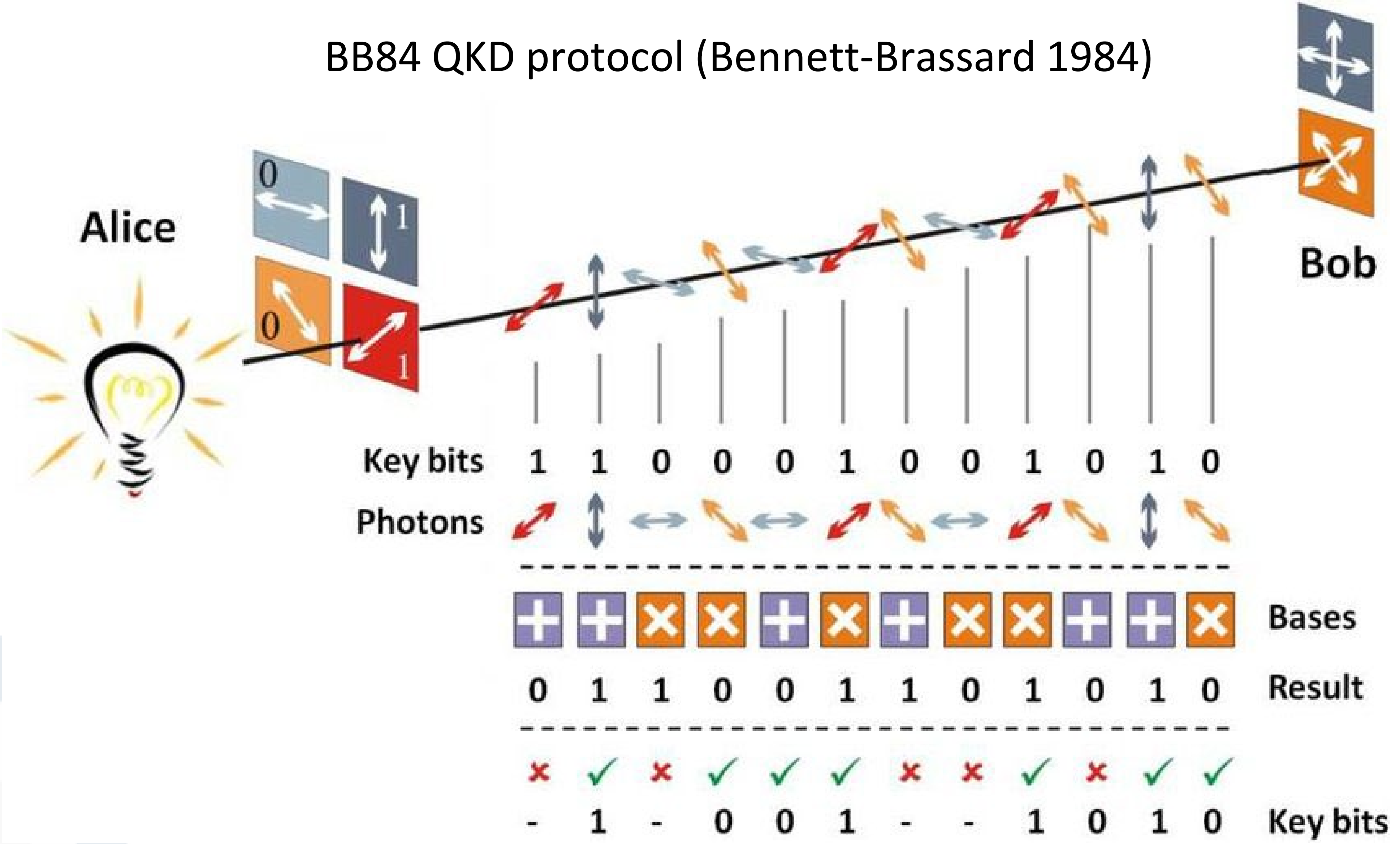


3. They publically reveal their choice of axes and discard pairs that don't match.

4. If remaining bits are perfectly correlated, then they are also secret.

Quantum key distribution (QKD)

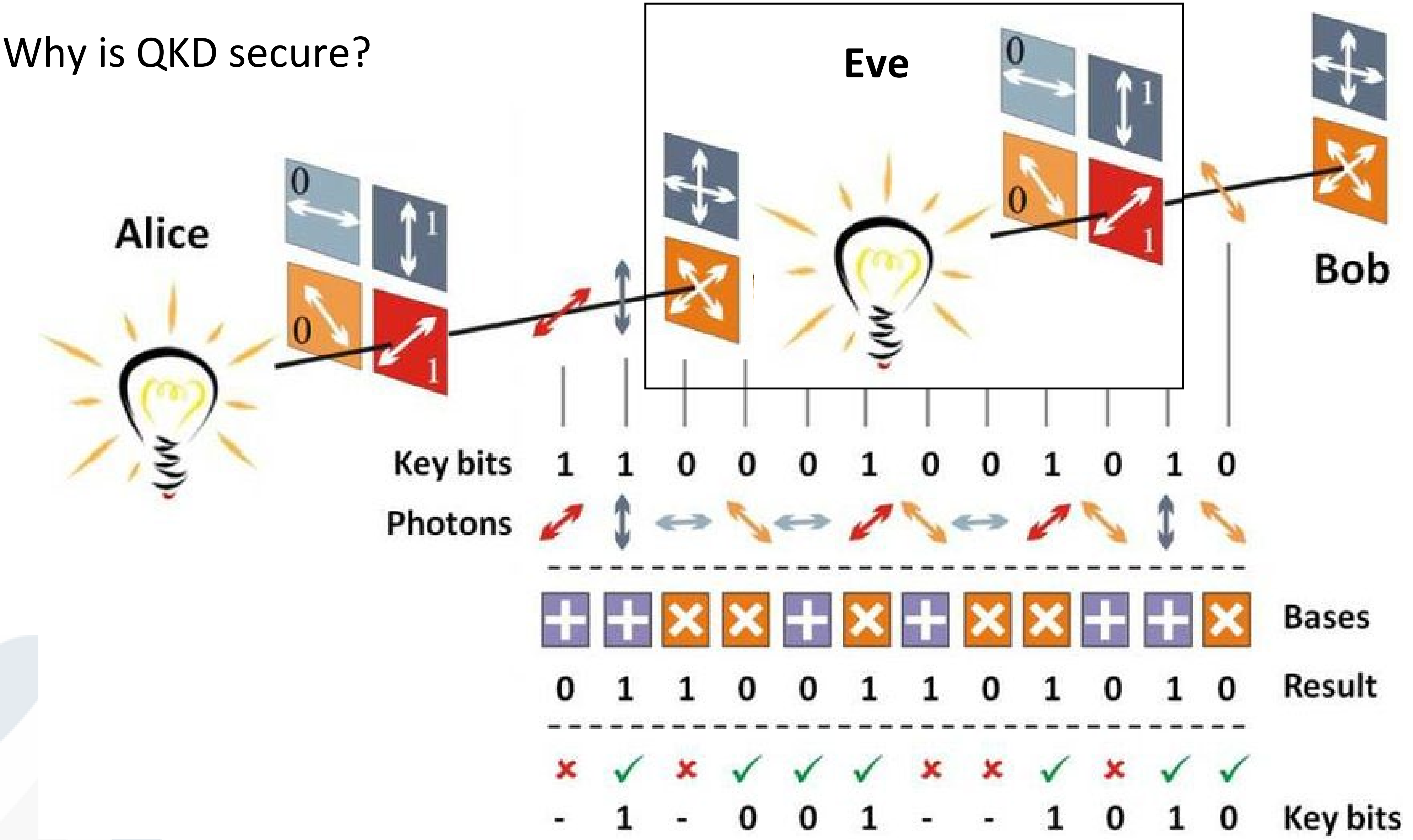
BB84 QKD protocol (Bennett-Brassard 1984)



Key bits	1	1	0	0	0	1	0	0	1	0	1	0
Photons	⤢	↕	↔	⤡	↔	⤢	⤡	↔	⤢	⤡	↕	⤡
Bases	+	+	×	×	+	×	+	×	×	+	+	×
Result	0	1	1	0	0	1	1	0	1	0	1	0
	✗	✓	✗	✓	✓	✓	✗	✗	✓	✗	✓	✓
Key bits	-	1	-	0	0	1	-	-	1	0	1	0

Quantum key distribution (QKD)

Why is QKD secure?



Key bits	1	1	0	0	0	1	0	0	1	0	1	0
Photons	⤢	↕	↔	⤡	↔	⤢	⤡	↔	⤢	⤡	↕	⤡
Bases	+	+	×	×	+	×	+	×	×	+	+	×
Result	0	1	1	0	0	1	1	0	1	0	1	0
	✗	✓	✗	✓	✓	✓	✗	✗	✓	✗	✓	✓
Key bits	-	1	-	0	0	1	-	-	1	0	1	0

Spanish plan on Quantum Communications

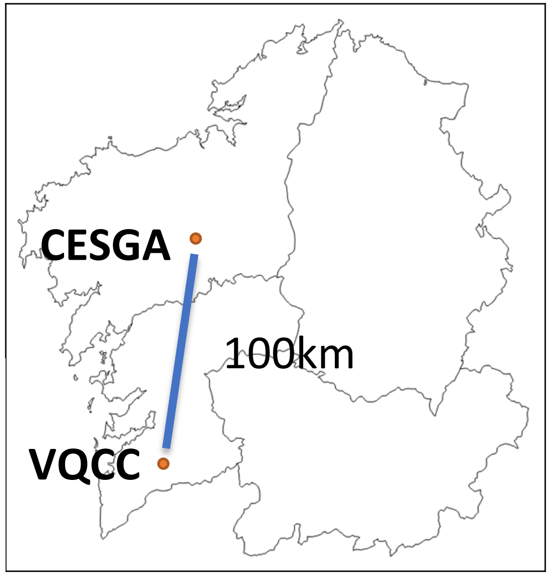
- **Goals**

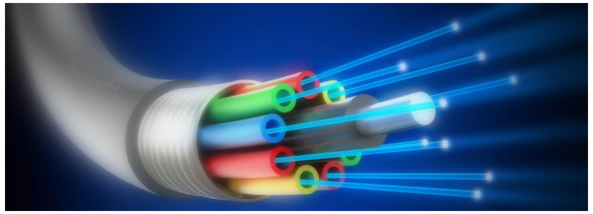
  1. **Set up a QKD fibered link between Santiago and Vigo**

     Current status:

     – Fibers VQCC-CESGA: up for tender
     – QKD equipment: preparing tender

Single long link





Financiado por la Unión Europea
NextGenerationEU
AXENCIA GALEGA DE INNOVACIÓN
GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN
Plan de Recuperación, Transformación y Resiliencia

Spanish plan on Quantum Communications

- **Goals**

1. **Set up a QKD fibered link between Santiago and Vigo**

   Current status:

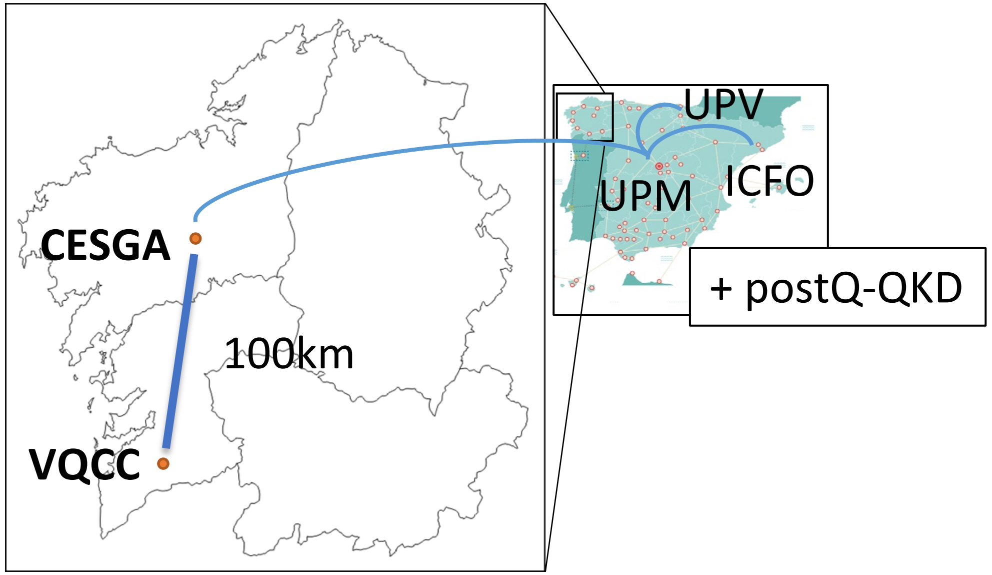
   – Fibers VQCC-CESGA: up for tender
   – QKD equipment: preparing tender

2. **Demostrate one use case**

   Currently exploring:

   i. GRADIANT: 5G/drones
   ii. UPM: transnational QKD+postquantum link

Single long link



Financiado por la Unión Europea
NextGenerationEU

AXENCIA GALEGA DE INNOVACIÓN

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

Plan de Recuperación, Transformación y Resiliencia

GRACIAS!

CESGA
GALICIA SUPERCOMPUTING CENTER

Quantum communications @ CESGA

Juan Villasuso

16
PLAN COMPLEMENTARIO DE
COMUNICACIONES
CUÁNTICAS
1ª REUNIÓN NACIONAL
Madrid, 19-21 de septiembre de 2023
Organizado por la Universidad Politécnica de Madrid
POLITÉCNICA

Iago Fernández

David Barral

Natalia Costas