

INTERCAMBIO DE CLAVE CUÁNTICO

ALICE Y BOB QUIEREN INTERCAMBIAR UNA CLAVE SUFICIENTEMENTE LARGA (DE 1's Y 0's) PARA PODER COMUNICAR POSTERIORMENTE POR UN CANAL INSEGURO USANDO EL CIFRADO DE VERNAM.

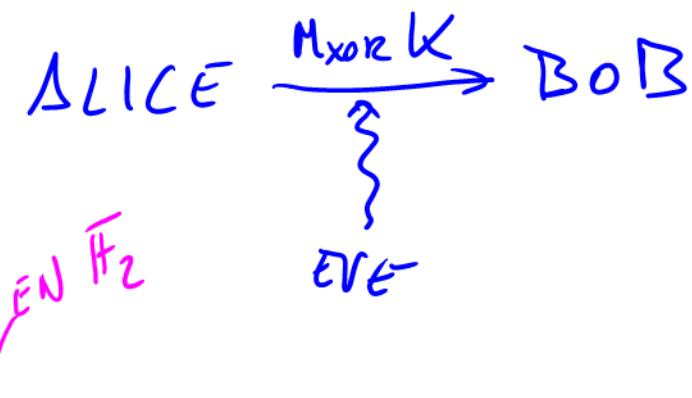
$$M = m_1, \dots, m_n \in \mathbb{F}_2^n$$

$$K = k_1, \dots, k_n \in \mathbb{F}_2^n$$

CIFRADO $C(M) = M \oplus K = m_1 + k_1, \dots, m_n + k_n$

DESCIFRADO $C(M) \oplus K = M$

CLAVE DE UN SOLO USO



¿COMO SE INTERCAMBIAN ALICE Y BOB UNA CLAVE
LARGA DE 0'S Y 1'S DE FORMA SEGURA?

OBJETIVO: INTERCAMBIAR UNA SECUENCIA CRIPTO-
GRAFICA DE BITS, ENTRE ALICE Y BOB, EN PRESEN-
CIA DE UN ADVERSARIO, EVE.

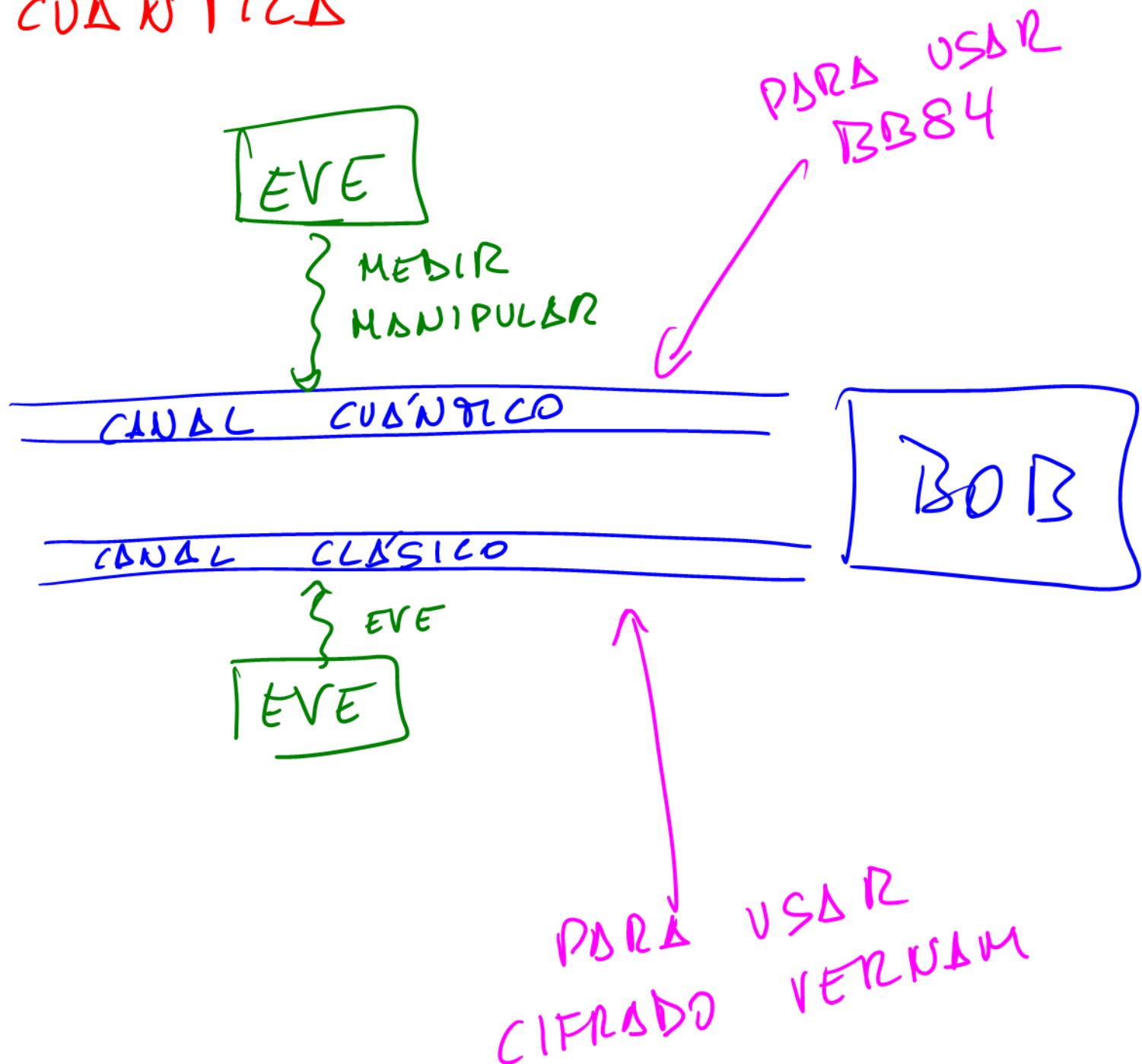
SUPOSICIÓN:

- TENEMOS UN CANAL PÚBLICO AUTENTIFICADO. ES DECIR LOS CONTENIDOS TRANSMITIDOS SON VISIBLES POR CUADQUIERA, PERO NO SE PUEDEN MODIFICAR O FALSIFICAR
- TENEMOS UN CANAL CUÁNTICO DONDE EVE PUEDE HACER CUALQUIER COSA QUE LE PERMITA LA

MECÁNICA CUÁNTICA

CUÁNTICA

Alice



POLARIZACIÓN DE LA LUZ

- LUZ (Y UNA ONDA ELECTROMAGNÉTICA) ES UNA VIBRACIÓN DEL CAMPO ELÉCTRICO, AYUD DIRECCIÓN DE VIBRACIÓN ES ORTOGONAL AL CAMINO DE LA LUZ.
- LA DIRECCIÓN DE VIBRACIÓN SE LLAMA POLARIZACIÓN DE LA LUZ.
- LA INTENSIDAD DE LA LUZ DECRECE CUANDO LA LUZ PASA A TRAVES DE UNA REJILLA (SLIT).
- CUANDO EL ÁNGULO ENTRE LA POLARIZACIÓN Y LA REJILLA ES DE 45° GRADOS, LA INTENSIDAD DE LA LUZ ES LA MITAD

EL ESTADO DE UN SISTEMA CUÁNTICO (POR EJEMPLO LA POLARIZACIÓN DE LA LUZ) SE REPRESENTA POR UN VECTOR DE LONGITUD 1 SOBRE EL CUERPO DE LOS NÚMEROS COMPLEJOS.

No somos NO VAMOS A USAR ESA NOTACIÓN PORQUE ES DEMASIADO SOFISTICADA PARA LOS PROPÓSITOS DE ESTE CURSO.

↳ SALVO EN LA PRÓXIMA TRANSPARENCIA

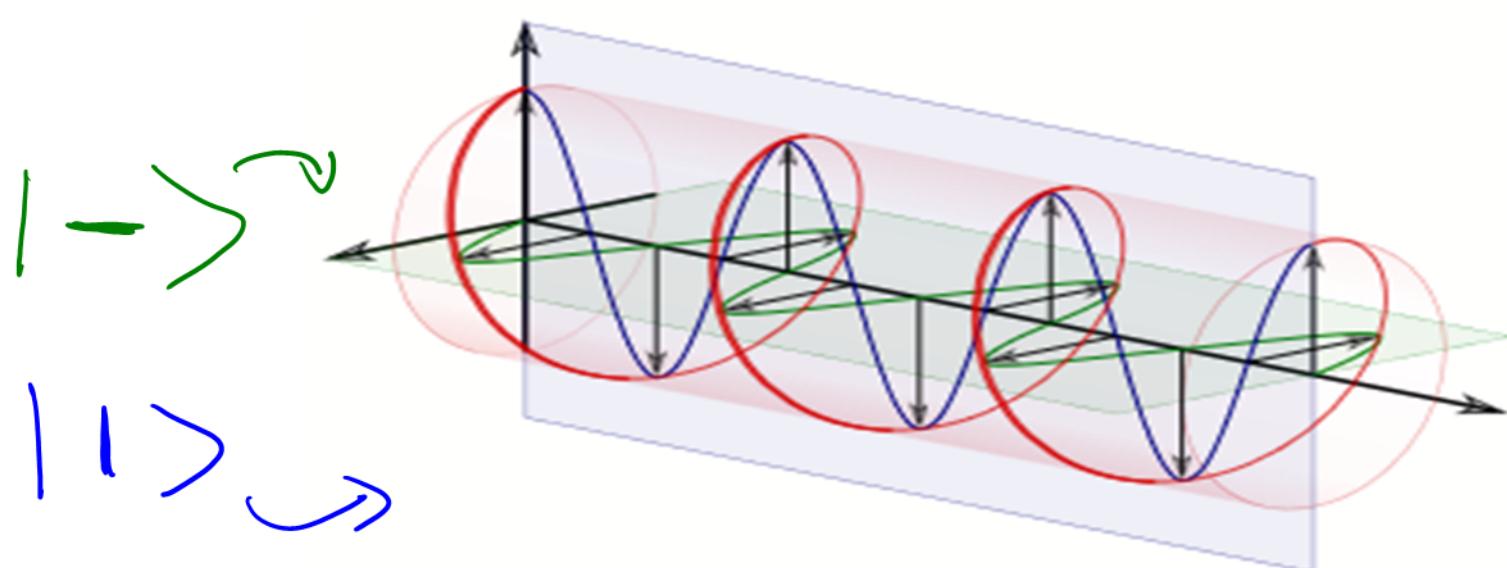
NOTACIÓN BRA-KET

$|\psi\rangle$ VECTOR COLUMNA

$\langle\psi|$ TRANSPUESTO CONJUGADO ($\langle\psi| = \overline{|\psi\rangle^T} = |\psi\rangle^*$)

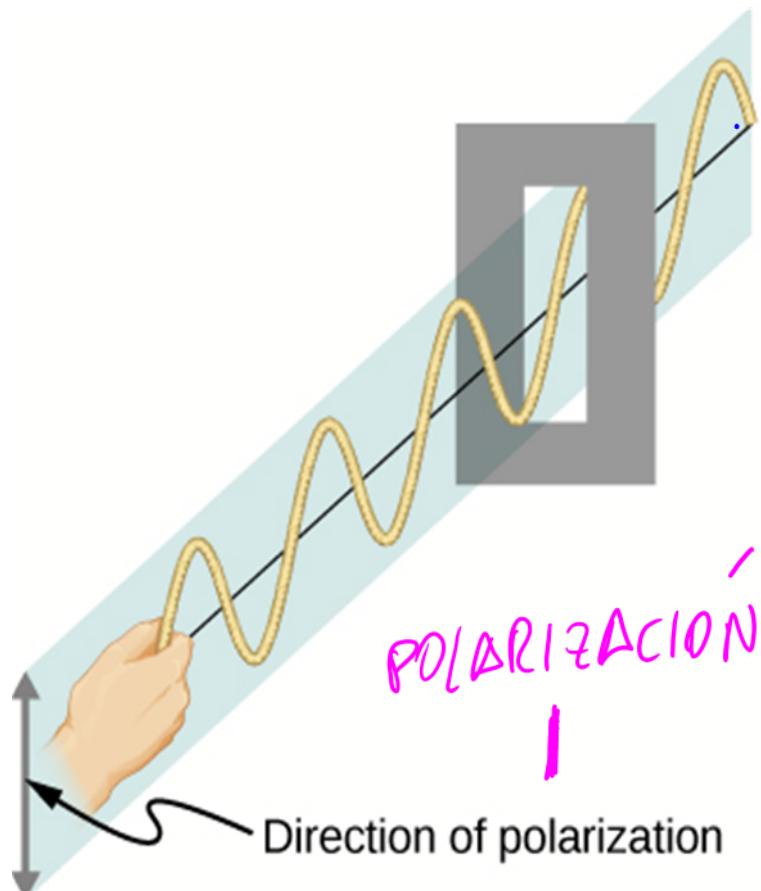
EJ $|-\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$, $|\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$ WIKIDEDIA
Y LIBRO

$$|\downarrow\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} = |+\rangle$$
 $|\diagdown\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |->$

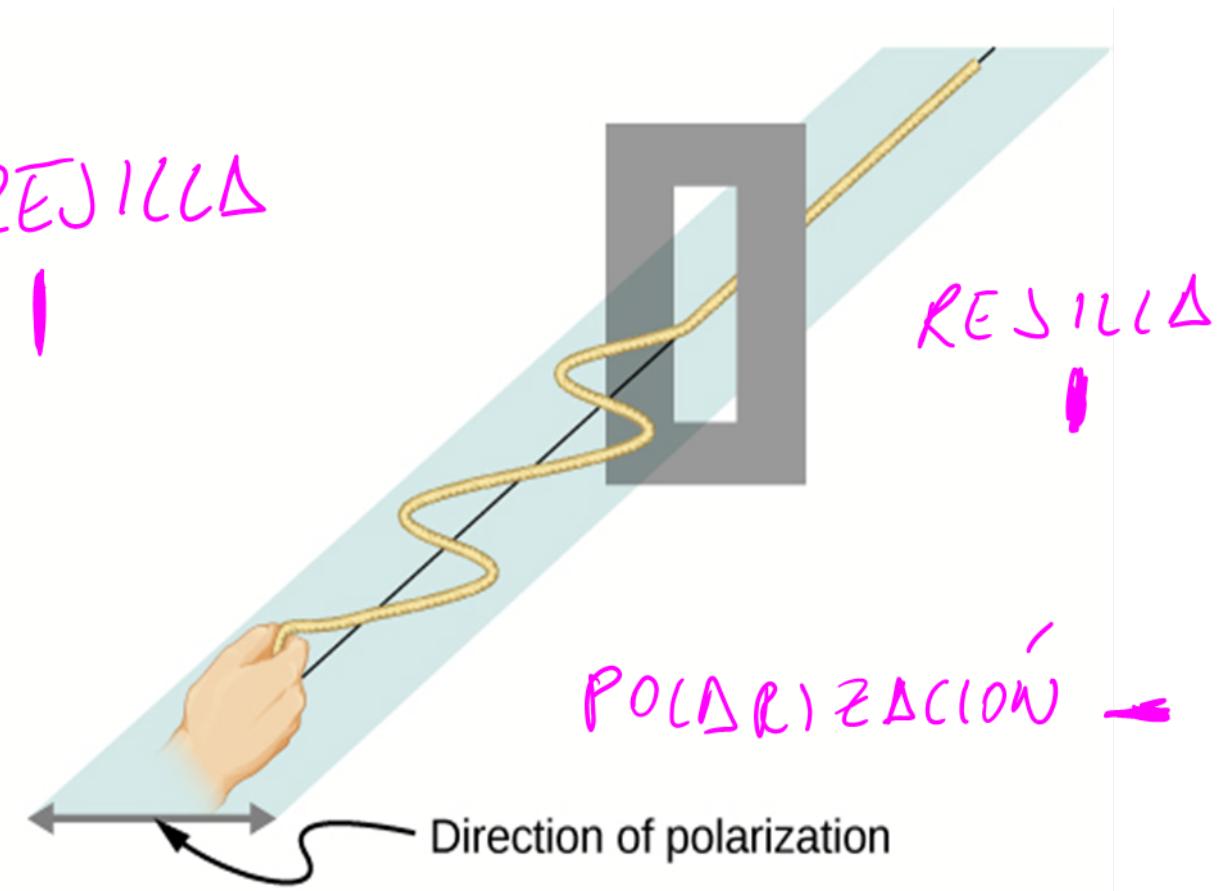


$\left\langle \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \right|$
POLARIZACIÓN
CIRCULAR

Y NOSOTROS QUITAMOS ' | ' > Y USAMOS - | / -



(a)



(b)

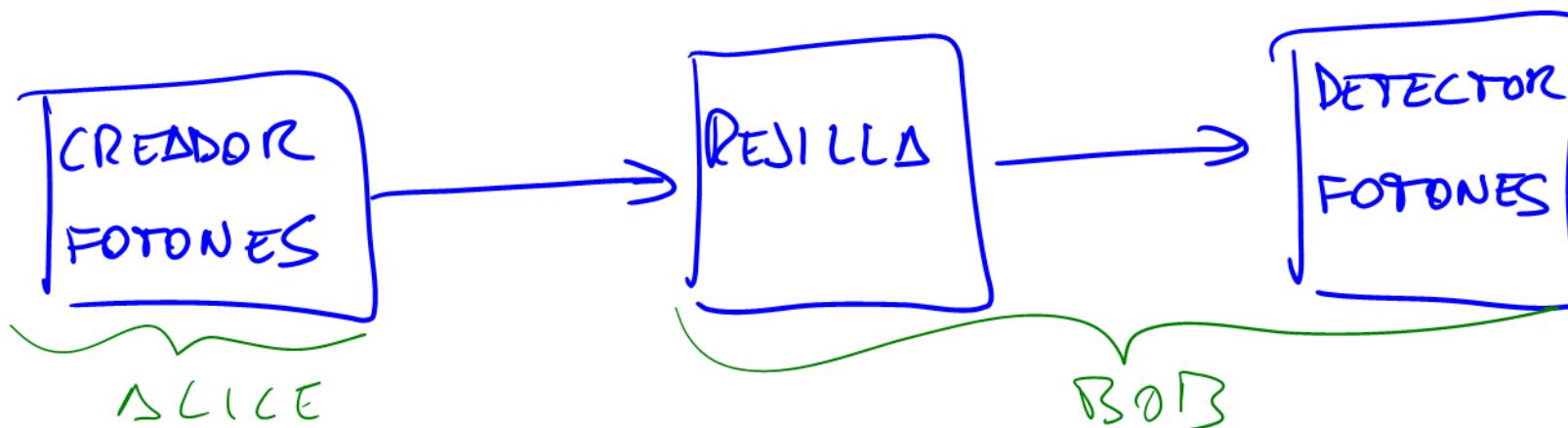
FOTOÓN

LA LUZ ES UNA ONDA. PERO A SU VEZ ES UNA COLECCIÓN DE PARCÍCULAS (COSAS DE FÍSICOS...) A CADA UNA DE ESTAS PARCÍCULAS SE LE LLAMA FOTOÓN

¿QUE PASA CUANDO UN FOTOÓN PASA POR UNA REJILLA?

DEPENDE DE LA DIRECCIÓN DE LA REJILLA Y DE LA POLARIZACIÓN DEL FOTOÓN, EN CONCRETO DE CUANTO DIFIEREN:

- SI DIFIEREN 45° : PASA CON PROBABILIDAD $\frac{1}{2}$
- SI SON PARALELAS (NO DIFIEREN): PASA CON PROBABILIDAD 1
- SI SON ORTOGONALES (DIFEREN 90°): PASA CON PROBABILIDAD 0



VAMOS A REPRESENTAR DE FORMA GRÁFICA
4 POLARIZACIONES (Y REJILLAS)

- | VERTICAL
- HORIZONTAL
- \\ } 45° INCLINACIÓN

PROTOCOLO BB84 (BENNET Y BRASSARD 1984)

Aquí presentaremos la versión original, que supone que el canal cuántico no tiene "ruido". Es decir, que no hay errores en la transmisión. Hay versiones modernas que pueden trabajar con ruido.

- 1) ALICE GENERA UNOS BITS DE FORMA ALATORIA, TANTOS COMO HAYA ACORDADO CON BOB.
- 2) ALICE CODIFICA CADA BIT GENERADO EN EL PASO ANTERIOR A UNA POLARIZACIÓN DE FOTOÓN

| BIT | 0 | 1 |
|---------|---|---|
| REGLA 1 | - | |
| REGLA 2 | / | \ |

ALICE ESCOGE 2 REGLAS
1 ó 2 AL AZAR PARA
CADA BIT

EJ:

BIT 0 1 0 0 1 0 1
REGLA 1 1 7 2 1 2 2

CODIFICACIÓN = 1 / 1 / 1 / 1

3) PARA CADA FOTOÓN, EL BOTÓN ESCOGE UNA REJILLA - ó / AL AZAR Y VE SI EL FOTOÓN ATRAVIESA O NO LA REJILLA.

4) EL BOTÓN ADIVINA LOS BITS TRANSMITIDOS USANDO ESTA TABLA

| REJILLA | POSA | ABSORBIDO |
|---------|------|-----------|
| - | 0 | 1 |
| / | 0 | 1 |

¿QUE PASA SI BOB NO USA LA REJILLA DE CUADRA?

ES DECIR, SI ALICE Y BOB NO USAN LA MISMA REGLA

- LA REJILLA HORIZONTAL NO DA NINGUNA
INFORMACIÓN ACERCA DEL BIT TRANSMITIDO
SI ALICE USÓ LA REGLA 2 PARA CODIFICARLO
- LA REJILLA DIAGONAL NO DA NINGUNA
INFORMACIÓN ACERCA DEL BIT TRANSMITIDO
SI ALICE USÓ LA REGLA 1 PARA CODIFICARLO

FOTO
POLARIZACIÓN

~~REJILLA~~ PASA $\frac{1}{2}$
ABSORBIDO $\frac{1}{2}$

5) ALICE Y BOB ANUNCIAN PÚBLICAMENTE LA REGLA DE POLARIZACIÓN Y REJILLA USADA PARA CADA BIT.

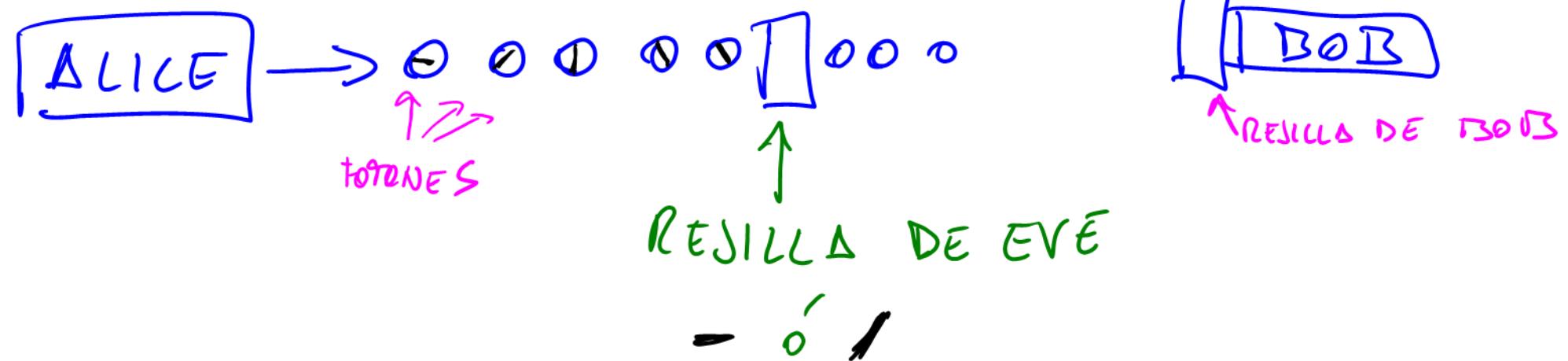
6) DESCARTAN TODOS LOS BITS PARA LOS CUALES:

- ALICE USO REGLA 1 PERO BOB USÓ REJILLA /
- ALICE USO REGLA 2 PERO BOB USÓ REJILLA //

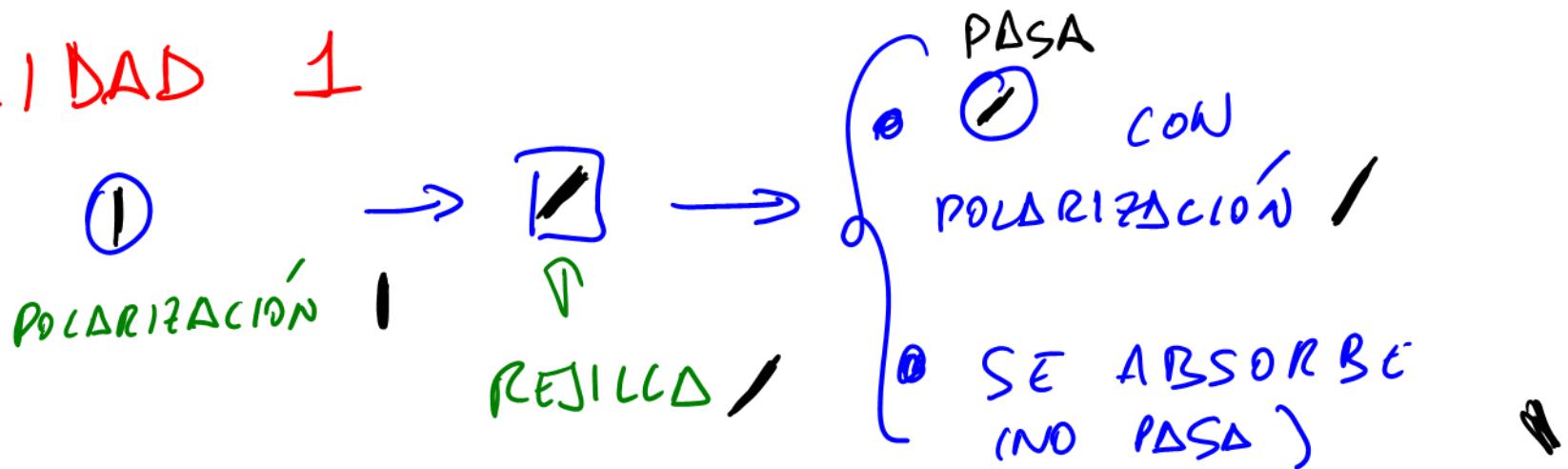
7) ALICE Y BOB ANUNCIAN PÚBLICAMENTE LA MITAD DE LOS BITS QUE NO HAN DESCARTADO. SI HAY UN ÚNICO BIT QUE NO COINCIDE, ABORTAN EL PROTOCOLO Y EMPIEZAN DESDE EL PRINCIPIO.

8) SI LA MITAD DE LOS BITS REVELADOS
COINCIDE, USAN LA OTRA MITAD COMO CLAVE

ESTRATEGIA DE EVE



LA REJILLA CAMBIA LA POLARIZACIÓN CON PROBABILIDAD 1



- 1) PARA CADA FOTÓN QUE EVE INTERCEPTA, EVE ESCOGE DE FORMA ALEATORIA UNA REJILLA - ó /
- 2) HACE PASAR EL FOTÓN POR LA REJILLA Y TRATA DE ADIVINAR EL BIT CODIFICADO DE LA MISMA FORMA QUE LO HACE BOB
- 3) SI EL FOTÓN ES ABSORBIDO, NECESA VOLVER A INYECTAR UN FOTÓN PARA QUE EL NÚMERO DE FOTONES QUE RECIBA BOB SEA EL ACORDADO POR ÉL Y ALICE.
¿QUÉ POLARIZACIÓN USA?
 - SI REJILLA - ABSORBE FOTÓN MANDA FOTÓN CON POLARIZACIÓN |

• SI REJILLA / ABSORBE FOTÓN MANDA FOTÓN
CON POLARIZACIÓN

¿POR QUÉ?

PORQUE ES LO MÁS PROBABLE

¿QUÉ PASA SI?

SI ALICE USA
REGLA 1 —

ELECCIÓN EQUIVOCADA

SI EVE USA
REJILLA /

ELECCIÓN CORRECTA

SI BOB USA
REJILLA —

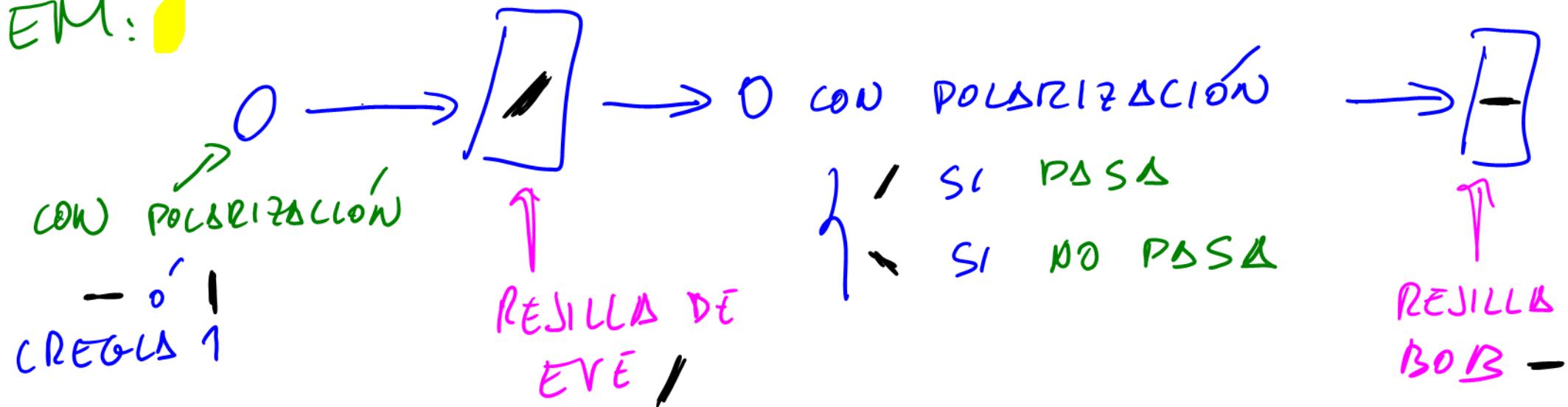
SI ALICE USA
REGLA 2 //

SI EVE USA
REJILLA —

SI BOB USA
REJILLA /

QUE ALICE Y BOB VAN A DETECTAR EL ATAQUE
DE EVE PARA ESE FOTOÓN CON PROBABILIDAD $\frac{1}{2}$

DEM:



EL FOTOÓN PASA POR LA RESILLA DE BOB
CON PROBABILIDAD $\frac{1}{2}$

{ SI PASA : 0 BOB ADIVINA
SI SE ABSORBE : 1

CON PROBABILIDAD $\frac{1}{2}$ BOB ADIVINA MÁS EL BIT
PERO DEBERÍA HABER ACERTADO CON PROBABILIDAD 1

SOBRE PASO 3)

¿POR QUÉ ALICE Y BOB ABORTAN?

- DEBERÍAN COINCIDIR TODOS LOS BITS CON PROBABILIDAD 1. PERO PUEDE PASAR, SIN QUE EVE INTERVenga, QUE NO COINCIDAN.

PROBABILIDAD 1 ≠ SUceso DETERMINISTA

PERO LO MÁS PROBABLE:

- PUEDE INDICAR QUE HAY UN CRIPTOANALISTA (EVE) INTERCEPTANDO LA COMUNICACIÓN.

¿CUANTOS BITS DEBE CONSIDERAR ALICE PARA OBTENER UNA CLAVE DE n BITS?

$(4+8)n$ ALICE (EN PASO 1)

↓
CON ALTA PROBABILIDAD QUEDAN 2^n BITS
AL MENOS

A BOB PORQUE LAS MITAD SON DESCARTADOS
AL NO USAR LA MISMA REGLA (PASO 6)

↓
LAS MITAD SE ANUNCIAN PÚBLICAMENTE (PASO 7)
PARA LA CLAVE QUEDAN n

PROBLEMAS DE ESTE PROTO COLO

- ESTAMOS SUPONIENDO QUE LAS POLARIZACIONES NO CAMBIAN DURANTE LA TRANSMISIÓN POR EL CANAL, ES DECIR, QUE LA COMUNICACIÓN NO TIENE ERRORES
- HEMOS SUPUESTO UNA ESTRATEGIA DE EVE QUE ES INTELIGENTE, PERO SIMPLE PERO PODRÍA HACER COSAS MÁS AVANZADAS CON LOS FOTONES. POR EJEMPLO, PODRÍA TRATAR DE COPIAR POLARIZACIONES EN SU ALMACÉN Y MEDIR SU POLARIZACIÓN DESPUÉS DE QUE ALICE ANUNCIE QUE REGLA HA USADO PARA CADA FOTÓN.
PERO
 - ES IMPOSIBLE COPIAR LA POLARIZACIÓN DE UNOS FOTONES QUE NO SE CONOCEN (NO CLONING THEOREM)
 - SI EVE ALMACENA LOS FOTONES SIN MEDIRLOS CESTO

ES POSIBLE) TIENE QUE ENVIAR A BOB UNOS FOTONES CREADOS POR ELLA CON UNA POLARIZACIÓN ALEATORIA. CUANDO ALICE Y BOB ANUNCIEN LA MITAD DE LOS BITS EN EL PASO 7) VA A HABER MUCHAS DISCREPANCIAS Y VAN A SORPRENDER

-ALICE Y BOB NO PUEDEN HACER DECRECER EL NÚMERO DE BITS VISTOS POR EVE A CASI CERO (UN NÚMERO TAN BAJO COMO QUIERAN)
POR EJEMPLO, SI EVE MIDE SÓLO 1 FOTÓN, ENTONCES EL NÚMERO MEDIO DE BITS DIVINADOS CORRECTAMENTE POR EVE (SIN QUE ALICE Y BOB SE DEN CUENTA) ES $\geq \frac{1}{8} = \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2}$

↑
REGISTRO
REGISTRO
RESILLA EVE

↑
REGISTRO
BOB

NOTA: UNA PROPUESTA AVANZADA DE ESTE PROTOCOLO SOLUCIONA LOS PROBLEMAS ANTERIORES

VENTAJAS:

- LA SEGURIDAD SE BASA EN LOS POSTULADOS DE LA MECÁNICA CUÁNTICA SIN EMBARGO, LA MAYORÍA DE PROTOCOLOS CRIPTOGRAFICOS CONVENCIONALES SE BASAN EN LA IMPOSIBILIDAD COMPUTACIONAL DE RESOLVER CIERTOS PROBLEMAS
- ES SEGURO FRENTE A UN ATAQUE CON UN ORDENADOR CUÁNTICO.

DESVENTAJAS

- LENTO : HASTA 100 MBITS / SEGUNDO
- CARO : AL MENOS 100.000 \$
- DISTANCIA LIMITADA : SE NECESITA UNA CONEXIÓN DIRECTA SIN REPETIDORES, LO CUAL LIMITA LA DISTANCIA ENTRE ALICE Y BOB A 200 KM. AUNQUE RECIENTEMENTE SE HAN CONSEGUIDO GRANDES AVANCES AL RESPECTO, ES ESPECIALMENTE EN CHINA, Y CADA VEZ ES MÁS BARATO

EJ: SE ENVÍAN 8 FOTONES Y 4 DE ELLOS SON INTERCEPTADOS POR EVE

| | | | | | | | | |
|-----------------------|----|----|----|----|----|----|----|----|
| FOTONES ENVIADOS | - | | / | \ | - | | / | \ |
| REJILLA DE EVE | - | - | | | / | | / | |
| REJILLA DE BOB | - | / | - | / | - | / | - | / |
| ANUNCIADOS EN β | NO | NO | NO | SI | NO | NO | NO | SI |

(O LOS PARES QUE NOS QUEDAN)

VAMOS A INCLUIR LA POSIBLE POLARIZACIÓN DE LOS FOTONES DESPUES DE LA MEDICIÓN DE EVE Y QUE FOTONES SON DESCARTADOS. TAMBIEN EL RESULTADO DE LA MEDICIÓN DE BOB.

FOTONES
ENVIADOS

- 0° | 1° / 0° \ 1° - 0° | 1° / 0° \ 1°

~~REJILLA
DE EVE~~

~~POLARIZACION
DESPUES EVE~~

REJILLA
DE BOB

- / - / - / - /

DESCARTADOS
EN 6)

D D D D

POSIBLE
RESULTADO
MEDICION BOB

Positivo
(+)

Abs.
(\)

Positivo
(+)

Abs.
(\)

BOB ADIVINA

0

1

0

1

~~SE DIFERENCIA
A EVE~~

CLAVE *

0

0

PRIMEROS
SUPONEMOS
QUE EVE
NO INTERCEPTA
NADA

| | |
|--------------------------------|--|
| FOTONES ENVIADOS | - $ ^0$ / $ ^0$ \ $=$ $ ^0$ / $ ^0$ \ |
| REJILLA DE EVE | - - / / |
| POLARIZACION DESPUES EVE | - / $\bar{ }^{1/2}$ - $\bar{ }^{1/2}$ / / / |
| REJILLA DE BOB | - / - / - / - / |
| POSIBLE RESULTADO MEDICION BOB | $P \Delta^{1/2} P_{1/2} \Delta^{1/2} P_{1/2} \Delta^{1/2} P \Delta^{1/2} P_{1/2} \Delta^{1/2} +$ |
| BOB ADIVINA | 0 $0^{1/2}$ $0^{1/2}$ $0^{1/2}$ 0 $0^{1/2}$ $0^{1/2}$ 1 |
| DESCARTADOS EN 6) | 0 D D $0^{1/2}$ 1 $1^{1/2}$ 0 D D 1 |
| SE DETECTA A EVE | SG DETECTADA NO SE DETECTA |
| CLAVE * | 0 |

*) SI EL ATAQUE DE EVE ES DETECTADO ENTONCES ALICE Y BOB ABORTAN EL PROTOCOLO y LO REINICIAN.

SI NO SE DETECTA A EVE, ENTONCES LA CLAVE ACORDADA POR ALICE Y BOB ES 00

PERO EVE NO OBTIENE NINGUN BIT DE LA CLAVE EN ESTE CASO

AHORA SUPONEMOS QUE LOS BITS
ANUNCIADOS SON LOS IMPARES

| | | | | | | | | | | | | | | | | | |
|--------------------------------|--|----------------|----------------|----------------|----------------|----------------|-----------|-----------|-----|----------------|----------------|----------------|----------------|----------------|----------------|----------------|--|
| FOTONES ENVIADOS | - $ ^0$ / $ ^0 \perp$ - $ ^0$ / $ ^0 \perp$ | | | | | | | | | | | | | | | | |
| REJILLA DE EVE | - - / / | | | | | | | | | | | | | | | | |
| POLARIZACION DESPUES EVE | - / $\bar{ }^{1/2}$ - $\bar{ }^{1/2}$ / / / | | | | | | | | | | | | | | | | |
| REJILLA DE BOB | - / - / - / - / | | | | | | | | | | | | | | | | |
| POSIBLE RESULTADO MEDICION BOB | <table style="margin-left: auto; margin-right: auto;"> <tr> <td>P</td> <td>$P_{1/2}$</td> <td>$P_{1/2}$</td> <td>$P_{1/2}$</td> <td>P</td> <td>$P_{1/2}$</td> <td>$P_{1/2}$</td> <td>A</td> </tr> <tr> <td>$\Delta_{1/2}$</td> <td>$\Delta_{1/2}$</td> <td>$\Delta_{1/2}$</td> <td>$\Delta_{1/2}$</td> <td>$\Delta_{1/2}$</td> <td>$\Delta_{1/2}$</td> <td>$\Delta_{1/2}$</td> <td></td> </tr> </table> | P | $P_{1/2}$ | $P_{1/2}$ | $P_{1/2}$ | P | $P_{1/2}$ | $P_{1/2}$ | A | $\Delta_{1/2}$ | |
| P | $P_{1/2}$ | $P_{1/2}$ | $P_{1/2}$ | P | $P_{1/2}$ | $P_{1/2}$ | A | | | | | | | | | | |
| $\Delta_{1/2}$ | $\Delta_{1/2}$ | $\Delta_{1/2}$ | $\Delta_{1/2}$ | $\Delta_{1/2}$ | $\Delta_{1/2}$ | $\Delta_{1/2}$ | | | | | | | | | | | |
| BOB ADIVINA | <table style="margin-left: auto; margin-right: auto;"> <tr> <td>0</td> <td>$0^{1/2}$</td> <td>$0^{1/2}$</td> <td>$0^{1/2}$</td> <td>0</td> <td>$0^{1/2}$</td> <td>$0^{1/2}$</td> <td>1</td> </tr> <tr> <td>$1^{1/2}$</td> <td>$1^{1/2}$</td> <td>$1^{1/2}$</td> <td>$1^{1/2}$</td> <td>$1^{1/2}$</td> <td>$1^{1/2}$</td> <td>$1^{1/2}$</td> <td></td> </tr> </table> | 0 | $0^{1/2}$ | $0^{1/2}$ | $0^{1/2}$ | 0 | $0^{1/2}$ | $0^{1/2}$ | 1 | $1^{1/2}$ | $1^{1/2}$ | $1^{1/2}$ | $1^{1/2}$ | $1^{1/2}$ | $1^{1/2}$ | $1^{1/2}$ | |
| 0 | $0^{1/2}$ | $0^{1/2}$ | $0^{1/2}$ | 0 | $0^{1/2}$ | $0^{1/2}$ | 1 | | | | | | | | | | |
| $1^{1/2}$ | $1^{1/2}$ | $1^{1/2}$ | $1^{1/2}$ | $1^{1/2}$ | $1^{1/2}$ | $1^{1/2}$ | | | | | | | | | | | |
| DESCARTADOS EN 6) | <table style="margin-left: auto; margin-right: auto;"> <tr> <td>0</td> <td>D</td> <td>D</td> <td>$i^{1/2}$</td> <td>0</td> <td>D</td> <td>D</td> <td>1</td> </tr> </table> | 0 | D | D | $i^{1/2}$ | 0 | D | D | 1 | | | | | | | | |
| 0 | D | D | $i^{1/2}$ | 0 | D | D | 1 | | | | | | | | | | |
| SE DETECTA A EVE | <table style="margin-left: auto; margin-right: auto;"> <tr> <td>NO</td> <td></td> <td></td> <td></td> <td>ANUNCIADOS</td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </table> | NO | | | | ANUNCIADOS | | | | | | | | | | | |
| NO | | | | ANUNCIADOS | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| CLOVG * | 0 1 CON PROB. $1/2$ Y 11 CON PROB. $1/2$ | | | | | | | | | | | | | | | | |

CON UNA PROB DE $1/2$ CLIC Y BOB
ESTÁN USANDO UNA CLAVE DIFERENTE

CON UNA PROB DE $1/2$ EVE SABE
"LA" CLAVE (A LO MEJOR ES DIFERENTE)