NO LOCALIDAD CUÁNTICA Y PROTOCOLOS QKD

Fundamentos de la no localidad cuántica y análisis de la seguridad en protocolos de QKD

9 de Enero de 2022

LAURA ALEJANDRA ENCINAR GONZÁLEZ

IÑAKI OTERO ANTERO

ÍNDICE

1. INTRODUCCIÓN

En este trabajo hablaremos en una primera parte sobre la no localidad cuántica: qué es, cómo se ha ido desarrollando a lo largo del tiempo y las principales consecuencias de este fundamento, como la paradoja de Einstein, Podolsky y Rosen o el Teorema de Bell. En una segunda parte, hablaremos de la seguridad en los protocolos de Quantum Key Distribution, y nos centraremos más adelante en uno de ellos que usa principios relacionados con la no localidad cuántica para su funcionamiento: el protocolo E91. Veremos cómo se implementa dicho protocolo usando el kit de desarrollo cuántico de Microsoft, y simularemos un ataque para comprobar la seguridad ante un intento de captar información por el canal cuántico.

2. NO LOCALIDAD CUÁNTICA

La no localidad cuántica es uno de los fundamentos más importantes de la mecánica cuántica. Este afirma que la mecánica cuántica no puede explicar sus resultados con teorías clásicas, debido a su naturaleza no realista. Esta afirmación no se realizó de la noche a la mañana, sino que lleva detrás de sí casi un siglo de discusiones científicas que continúan hoy en día.

La mecánica cuántica siempre ha sido un tema de enorme misterio y controversia en la ciencia. Muchas interpretaciones hechas por diferentes científicos se han publicado a lo largo de los años, pero sin duda una de las más aceptadas hasta ahora es la conocida como interpretación de Copenhague. Está atribuida a Niels Bohr y Werner Heisenberg y fue desarrollada entre los años 1925 y 1927, y a día de hoy es una de las interpretaciones que más se usa en la enseñanza. Además de explicar que la mecánica cuántica es intrínsecamente indeterminista, esta interpretación expone por primera vez la regla de Born, que afirma que la función de onda de un sistema contiene probabilidades que influyen en el resultado de las mediciones de dicho sistema. Dicha función de onda colapsa a un posible resultado al hacer una medición, eliminando todos los demás.

Sin embargo, la interpretación de Copenhague tenía algunos críticos, y entre ellos se encontraban Albert Einstein, Boris Podolsky y Nathan Rosen, quienes mediante una paradoja intentaron exponer la falta de completitud de la interpretación de Copenhague [1].

2.1 Paradoja de Einstein, Podolsky y Rosen

Mediante un experimento publicado en 1935, Einstein, Podoslky y Rosen intentaron demostrar que la mecánica cuántica no podía ser considerada completa. Este experimento consideraba un par de electrones en el estado $|\varphi\rangle$, siendo este:

$$|\varphi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B) = \frac{1}{\sqrt{2}}(|+\rangle_A|-\rangle_B - |-\rangle_A|+\rangle_B),$$

siendo A y B dos partículas diferentes [2]. Lo que afirma este estado es que tenemos dos electrones entrelazados que sabemos que tienen espines opuestos, pero que no sabemos qué espín tiene cada uno hasta que lo midamos. Por ejemplo, si medimos el electrón A y obtenemos un $|1\rangle$, entonces podremos predecir el resultado del electrón B, que será $|0\rangle$. Dada esta definición y haciendo asunciones de "localidad" (implica que eventos que se dan muy lejos uno del otro puedan afectarse entre ellos) y "realidad" (los estados de los elementos físicos existen antes de ser medidos), Einstein, Podolsky y Rosen razonan lo siguiente:

1. Si se puede predecir con certeza el resultado de una medición sin alterar el objeto medido, entonces debe haber un elemento de la realidad correspondiente a ese resultado, suponiendo que la mecánica cuántica es realista.
2. Asumiendo que la mecánica cuántica es local, es posible medir el espín del electrón A, que se encuentra en el estado $|\varphi\rangle$, sin afectar al electrón B.

3. Si medimos el espín del electrón A, entonces sabremos con certeza cuál es el espín del electrón B.
4. Por tanto, cuando los electrones se encuentran en el estado $|\varphi\rangle$, el electrón B tiene un espín definido antes de ser medido, que no ha sido alterado debido a la asunción de localidad y que podemos predecir con certeza.
5. Aun así, la definición del estado $|\varphi\rangle$ no representa con certeza el espín del electrón B.
6. Por tanto, o la descripción de la mecánica cuántica según la interpretación de Copenhague es incompleta, o viola el principio de propagación finita de los efectos físicos (los efectos de una medición no pueden viajar más rápido que la velocidad de la luz, descrito en la teoría de la relatividad especial, escrita por Einstein).

Tras esta refutación, Einstein, Podolsky y Rosen proponen buscar una teoría local y realista basada en dos hipótesis: que estos electrones ya tienen un espín definitivo en cada dirección en el momento que son producidos, y que los efectos de las acciones sean locales y cumplan el principio de propagación finita de los efectos físicos. Además, dejan en el aire la existencia de una teoría de variables ocultas, de forma que todo el rango estadístico de las posibles soluciones ante una medición quedase reflejado y pudiese ser determinista, aunque nunca llegaron a proponer cuál era [3].

2.2 Teorema de Bell

En 1964, John Stewart Bell publicaba su artículo "Sobre la paradoja Einstein Podoslky Rosen", en la que respondía a la incógnita que dejaban en el aire estos tres científicos: si existía una teoría de variables ocultas locales que pudiera definir la mecánica cuántica. En el conocido como teorema de Bell, decía lo siguiente: "Ninguna teoría física de variables ocultas locales puede reproducir todas las predicciones de la mecánica cuántica". Para afirmar esto, Bell se basó en una desigualdad deducida por él mismo, que mostraba que una hipótesis de variables locales ocultas lleva a unas restricciones en la correlación de los resultados de las diferentes mediciones, y si estas restricciones son violadas, la realidad no podrá ser descrita por una teoría de variables locales ocultas. La desigualdad original de Bell es la siguiente:

$$1 + C(b,c) \geq |C(a,b) - C(a,c)|,$$

donde C es la correlación de pares de partículas y a,b y c son los ajustes del aparato con los que se emiten las partículas [4].

Para ver un ejemplo del teorema de Bell, vamos a ver el siguiente ejemplo.

Supongamos que vamos a medir el espín de nuestros electrones entrelazados en 3 direcciones: 0º, 60º y 120º. Sabemos que la probabilidad de desacuerdo originada al medir los espines de ambos electrones en la dirección misma dirección es de 1, ya que por la definición dada anteriormente, si el espín del primer electrón está orientado hacia arriba ($|0º - up\rangle$), el espín del segundo estará orientado en la dirección contraria ($|0º - down\rangle$). ¿Pero qué ocurre si medimos el espín del primer y segundo electrón con direcciones diferentes? No estaremos midiendo la misma propiedad de espín, pero sabemos que va a haber cierta correlación entre los resultados.

Pongamos el ejemplo de medir el espín de 0º en el primero y el espín de 120º en el segundo. Al medir el primer electrón, tenemos que la probabilidad de que esté orientado hacia arriba es la misma que de que lo esté hacia abajo, de 0'5. Suponiendo que el espín del primer electrón es $|0º - down\rangle$, sabremos a ciencia cierta que el espín del segundo electrón es $|0º - up\rangle$. Pero nosotros queremos ver el espín de 120º, por lo que llevaremos a cabo algunas operaciones para hallar qué probabilidad tiene de están hacia arriba o hacia abajo.

El vector de estado de un electrón con espín $|120º - up\rangle$ es $\binom{1/2}{\sqrt{3}/2}$, mientras que el del espín $|0º - up\rangle$ es $\binom{1}{0}$. Usando una fórmula para conseguir la probabilidad de los espines para diferentes ángulos:

$$P(spin\ up, 120º) = \langle 120º - up|0º - up\rangle^2 = (\begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix} \cdot \binom{1}{0})^2 = \frac{1}{4}$$

Por tanto, la probabilidad de que sea $|120º - up\rangle$ es de ¼, mientras que la de $|120º - down\rangle$ es de ¾. En otras palabras, la probabilidad de acuerdo con la primera medición es de ¾, mientras que la de desacuerdo es de ¼. Si hacemos lo mismo para todas las posibles permutaciones de este caso, obtendremos la siguiente tabla.

Propiedad de espín		Probabilidad de desacuerdo
Electrón 1	Electrón 2	
0º	0º	1
0º	60º	¾
0º	120º	¼
60º	0º	¾
60º	60º	1
60º	120º	¾
120º	0º	¼
120º	60º	¾
120º	120º	1

Esta tabla muestra los resultados basados en la mecánica cuántica con la interpretación de Copenhague, pero nosotros queremos obtener los mismos resultados dando un valor concreto a cada uno de los espines, o lo que es lo mismo, queremos ver si estos resultados se pueden dar generando una teoría de variables locales ocultas.

Para ello, primero vamos a generar todas las posibles combinaciones de espines para los dos electrones. Si nos fijamos las combinaciones de arriba son opuestas a las de abajo, por lo que las vamos a tratar como si fueran la misma.

	Profile (a1)		Profile (b1)		Profile (c1)		Profile (d1)	
	Elect. 1	Elect. 2	Elect. 1	Elect. 2	Elect. 1	Elect. 2	Elect. 1	Elect. 2
0° spin	↑	⇓	↑	⇓	↑	⇓	⇓	↑
60° spin	↑	⇓	↑	⇓	⇓	↑	↑	⇓
120° spin	↑	⇓	⇓	↑	↑	⇓	↑	⇓
	Profile (a2)		Profile (b2)		Profile (c2)		Profile (d2)	
	Elect. 1	Elect. 2	Elect. 1	Elect. 2	Elect. 1	Elect. 2	Elect. 1	Elect. 2
0° spin	⇓	↑	⇓	↑	⇓	↑	↑	⇓
60° spin	⇓	↑	⇓	↑	↑	⇓	⇓	↑
120° spin	⇓	↑	↑	⇓	⇓	↑	⇓	↑

Lo siguiente será definir cuatro variables: *a*, *b*, *c* y *d*. Estas mostrarán con qué frecuencia se dan las combinaciones de arriba: a para las combinaciones a1 y a2, b para las combinaciones b1 y b2, etc.

Por último, vamos a generar unas ecuaciones en base a los datos que ya tenemos. En primer lugar, sabemos que la suma de todas las combinaciones posibles será 1, algo trivial en estadística.

Después, podemos comprobar que las combinaciones a1, a2, b1 y b2 tienen desacuerdo al medir los espines sobre las direcciones de 0º y 60º y esto ocurre un 75% de las veces que se miden ambos electrones. Lo mismo ocurre con las combinaciones a1, a2, c1 y c2 y los espines de 0º y 120º, y con las combinaciones a1, a2, d1 y d2 y los espines de 60º y 120º, ocurriendo un 25% y un 75% de las veces respectivamente. Juntando todo esto, podemos definir el siguiente sistema de ecuaciones:

$$\begin{cases} a+b+c+d=1 \\ a+b=3/4 \\ a+c=1/4 \\ a+d=3/4 \end{cases}$$

La solución a este sistema de ecuaciones da los siguientes valores a las frecuencias de nuestras combinaciones: $a=\frac{3}{8}, b=\frac{3}{8}, c=-\frac{1}{8}, d=\frac{3}{8}$. Como bien sabemos, es físicamente imposible que la frecuencia de que ocurra un evento sea negativa, un suceso no puede ocurrir una cantidad negativa de veces. Esto deja en evidencia que es imposible conseguir un modelo matemático de variables ocultas locales que consiga emular el comportamiento de la mecánica cuántica [5].

En resumen, Bell demostró que Einstein, Podolsky y Rosen estaban equivocados, y gracias a sus experimentos, probó inequívocamente que las ecuaciones que restringen las variables locales (conocidas como desigualdades de Bell) son violadas en la mecánica cuántica, mostrando que el realismo local en esta es imposible y dejando abierta el misterio de la no localidad cuántica. Descubrimientos más recientes como el teorema de no comunicación prueban que la no localidad cuántica no rompe con la relatividad especial, probando que la información no se puede transmitir a una velocidad mayor que la de la luz, lo que en cierto sentido da un ápice de localidad a la mecánica cuántica. Lo que está claro es que, por el momento, la no localidad cuántica seguirá generando debates en la comunidad científica, como lleva ocurriendo durante años.

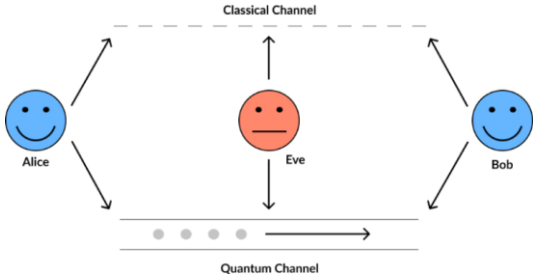
3. SEGURIDAD EN PROTOCOLOS QKD

Los protocolos cuánticos de distribución de claves, denominados QKD (Quantum Key Distribution), presentan un avance en la distribución segura de claves privadas gracias a la utilización de un canal cuántico. De esta manera, se garantiza que un espía no puede extraer información sin hacer notar su presencia, ya que los estados cuánticos no se pueden clonar y al realizar una medición sobre este, queda modificado. A pesar de ello, estos protocolos presentan ciertas vulnerabilidades y por tanto, posibles ataques.

En este proceso de distribución de claves se utilizará un canal cuántico para enviar fotones y un canal clásico para reconciliar y depurar la información. Para esquematizar dicho proceso llamaremos al emisor de la clave Alice, al receptor Bob y al espía Eve, todos ellos tendrán acceso a ambos canales.

3.1 Seguridad en protocolos basados en el teorema de no-clonación

En los protocolos basados en el teorema de no-clonación, entre los que se encuentran el BB84, el B92 o el SARG04, Alice enviará bits de información codificados en fotones polarizados a través del canal cuántico y Bob deberá interpretarlos usando diferentes bases, que después se cotejarán a través del canal clásico.



1. Representación general de una configuración QKD

La seguridad en este tipo de protocolos se basa en comprobar parte de la clave a través del canal clásico y rechazarla si se encuentran discrepancias, ya que podría suponer la presencia de un espía. El problema se manifiesta cuando llevamos este sistema a la práctica, entonces pueden aparecer errores debidos a imperfecciones técnicas o a cambios de temperatura que producen discrepancias sin conllevar la presencia de un espía. Para determinar si las discrepancias se deben a un espía o a otra causa es importante determinar una cota de error, a partir de la cual se abortaría el proceso.

Una de las estrategias de ataque que se utiliza es la denominada Interceptar-Reenviar. En este ataque Eve intercepta el fotón enviado por Alice, realiza la medición del qubit recibido utilizando una base (elegida de forma aleatoria o utilizando siempre una base que maximice la probabilidad de acierto), guarda el resultado y envía el qubit resultante (modificado) a Bob. Después, mediante la información que se comparte en por el canal clásico, Eve conservará sólo los bits correspondientes con la clave. Por ejemplo, en caso del protocolo BB84 conservará sólo los bits correspondientes a las posiciones en las que Alice y Bob han usado la misma base.

Para ver que impacto tiene esta estrategia en la seguridad del protocolo BB84, vamos a calcular la probabilidad de coincidencia entre los bits de Alice y los bits de Eve. Sea a el bit de Alice, a' el bit de Eve una vez realizada la medida y a'' el bit de Bob, sea B la base usada por Alice y Bob y B' la base usada por Eve y considerando que Eve elige entre una de las dos bases aleatoriamente:

$$P(a=a') = P(a=a'/B=B')\,P(B=B') + P(a=a'/B\neq B')\,P(B\neq B') = 1\cdot 0.5 + 0.5\cdot 0.5 = 0.75$$

Calculamos también la probabilidad de coincidencia entre los bits de Alice y Bob:

$$P(a=a'') = P(a=a''/B=B')\,P(B=B') + P(a=a''/B\neq B')\,P(B\neq B') = 1\cdot 0.5 + 0.5\cdot 0.5 = 0.75$$

De estos resultados obtenemos que la cadena de Eve tendrá el 75% de aciertos y la discrepancia introducida en la clave de Bob sólo será del 25%. Por lo que la cota de error deberá estar por debajo del 25% para poder detectar este tipo de ataque.

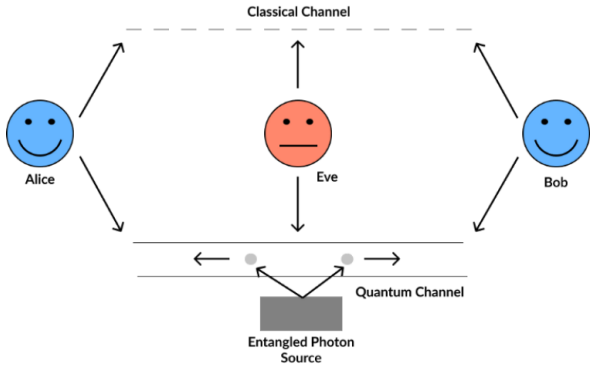
Otro de los ataques que Eve puede utilizar son los denominados PNS (Photon Number Splitting) basado en pulsos con dos fotones. Esta estrategia consiste en separar los dos fotones del pulso, enviar uno de ellos a Bob y conservar el otro en una memoria cuántica, una vez terminada la fase de reconciliación de bases se realizará la medición en la base correspondiente. Este ataque es posible gracias a la dificultad de enviar fotones individualmente cuando llevamos este tipo de protocolos a la práctica. En el año 2000, se realizó un experimento que demostraba la viabilidad de la distribución cuántica de clave usando fibra óptica, pero en dicho experimento se comprobó que el 28% de los pulsos enviados detectables contenían dos o más fotones [6].

3.2 Seguridad en protocolos basados en pares EPR

Protocolos como el E91 basan su seguridad en la utilización de pares EPR, es decir de pares de qubits entrelazados. De esta manera, se garantiza que realizando la medida en las mismas bases,

Alice y Bob obtendrán resultados idénticos siempre que el entrelazamiento permanezca estable y un espía no haya modificado el estado.

En este caso, en lugar de utilizar el canal cuántico para enviar qubits desde Alice hasta Bob, se utiliza para enviar cada qubit de un par entrelazado desde una fuente hasta Alice y Bob. Es posible eliminar este canal si Alice y Bob crean el par EPR estando físicamente ubicados en el mismo lugar, evitando de este modo un potencial vector de ataque.



2. Representación de la configuración del protocolo E91

Otra ventaja con respecto a la seguridad del protocolo es que, a diferencia de en los protocolos BB84 y B92, no se necesita crear información clásica para después codificarla en qubits. En su lugar, los bits 0 y 1 aparecen de manera equiprobable al realizar la medida en cada parte del par entrelazado, proporcionando verdadera aleatoriedad a la clave. Como explica Ekert, creador del protocolo E91, la clave no existe hasta que Alice y Bob realizan las mediciones y comparan las bases, por lo que Eve no puede obtener ninguna información de las partículas que viajan desde la fuente hasta uno de los usuarios legítimos [7]. Aún así, es posible que Eve inserte su propio qubit en el proceso (por ejemplo, durante la creación del par EPR). Para detectar este ataque Ekert propuso usar una prueba de la desigualdad de Bell.

4. IMPLEMENTACIÓN DEL PROTOCOLO E91 Y SIMULACIÓN DE UN ATAQUE

Para realizar esta implementación en Q# del protocolo hemos utilizado el kit de desarrollo cuántico de Microsoft (QDK) [8], mediante su extensión para Visual Studio Code [9]. También necesitaremos las siguientes librerías, incluidas en QKD:

```
open Microsoft.Quantum.Intrinsic;     // for the H operation
open Microsoft.Quantum.Random;   // for DrawRandomBool
open Microsoft.Quantum.Arrays;   // for Chunks
open Microsoft.Quantum.Convert;   // for RangeAsIntArray
```

Comenzamos creando la operación correspondiente al protocolo, e inicializando los arrays donde se guardarán los resultados de las mediciones y las bases utilizadas.

```
operation RunEPRQKDProtocol(expectedKeyLength : Int, eavesdropperProbability : Double) : Bool {

    mutable aliceResults = new Bool[0];
    mutable aliceBases = new Bool[0];

    mutable bobResults = new Bool[0];
    mutable bobBases = new Bool[0];
```

Para el siguiente paso, crearemos 4n+δ pares EPR, siendo n la longitud de la clave deseada. Esto se debe a que se descartarán aproximadamente el 50% de los qubits al realizar la comprobación de bases, otro 50% se deberá revelar para comprobar que no existe un espía y el δ restante dejará un margen de seguridad. En este caso en el que queremos obtener una clave de 256 bits, escogeremos δ=64.
En este fragmento de código también se contempla la posibilidad de realizar un ataque, ya que Eve puede interceptar uno de los qubits pertenecientes al par antes de que este llegue a Bob. En este momento dejamos que Eve realice una medición (eligiendo una base arbitrariamente) sobre el qubit de Bob. De esta medición Eve no obtendrá ninguna información sobre la clave a no ser que las bases elegidas coincidan con las que elijan en común Alice y Bob.

```
for i in 0..(4 * expectedKeyLength + 64) {
    use (aliceQubit, bobQubit) = (Qubit(), Qubit()) {

        // create entanglement between aliceQubit and bobQubit
        H(aliceQubit);
        CNOT(aliceQubit, bobQubit);

        // determine if eavesdropper should jump in
        // if so, let Eve interact with the qubit of Bob
        let shouldEavesdrop = DrawRandomBool(eavesdropperProbability);
        if (shouldEavesdrop) {
            let eveBasisSelected = DrawRandomBool(0.5);
            let eveResult = Measure([eveBasisSelected ? PauliX | PauliZ], [bobQubit]);
        }

        // Alice and Bob choose a random basis by drawing a random bit
        // 0 will represent {|0>,|1>} computational (PauliZ) basis
        // 1 will represent {|->,|+>} Hadamard (PauliX) basis
        let (aliceBase, aliceResult) = MeasureInRandomBasis(aliceQubit);
        set aliceBases += [aliceBase == PauliX];
        set aliceResults += [aliceResult];

        let (bobBase, bobResult) = MeasureInRandomBasis(bobQubit);
        set bobBases += [bobBase == PauliX];
        set bobResults += [bobResult];
    }
}
```

Para que Alice y Bob realicen la medida de los qubits eligiendo bases de forma aleatoria se crea el siguiente método, que elige la base Pauli Z {|0⟩,|1⟩} o Pauli X {|+⟩,|−⟩} en base al resultado de DrawRandomBool(0.5).

```
operation MeasureInRandomBasis(qubit : Qubit) : (Pauli, Bool) {
    let basisSelected = DrawRandomBool(0.5) ? PauliX | PauliZ;
    let aliceResult = Measure([basisSelected], [qubit]);
    let classicalResult = ResultAsBool(aliceResult);
    Reset(qubit);
    return (basisSelected, classicalResult);
}
```

En el siguiente paso se comparan las bases elegidas por ambos y se mantienen sólo aquellas en las que hayan coincidido.

```
mutable aliceResultsAfterBasisComparison = new Bool[0];
mutable bobResultsAfterBasisComparison = new Bool[0];

// compare bases and pick shared results
for i in 0..Length(aliceResults)-1 {
    // if Alice and Bob used the same basis
    // they can use the corresponding bit
    if (aliceBases[i] == bobBases[i]) {
        set aliceResultsAfterBasisComparison += [aliceResults[i]];
        set bobResultsAfterBasisComparison += [bobResults[i]];
    }
```

```
}
```

A continuación, se realiza la comparación de la mitad de los bits restantes para comprobar si Eve ha intervenido en el proceso, aceptando una cota de error en este caso del 10%. Si las discrepancias encontradas al llevar a cabo esta comparación superan la cota de error se abortará el proceso, en caso contrario se continuará con el protocolo.

```
Message("Performing eavesdropping check....");
// select a random bit of every 2 bits for eavesdropping check
mutable eavesdropppingIndices = new Int[0];
let chunkedValues = Chunks(2, RangeAsIntArray(IndexRange(aliceResultsAfterBasisComparison)));
for i in IndexRange(chunkedValues) {
    if (Length(chunkedValues[i]) == 1) {
        set eavesdropppingIndices += [chunkedValues[i][0]];
    } else {
        set eavesdropppingIndices += [DrawRandomBool(0.5) ? chunkedValues[i][0] |
chunkedValues[i][1]];
    }
}

// compare results on eavesdropping check indices
mutable differences = 0;
for i in eavesdropppingIndices {
    // if Alice and Bob get different result, but used same basis
    // it means that there must have been an eavesdropper
    if (aliceResultsAfterBasisComparison[i] != bobResultsAfterBasisComparison[i]) {
        set differences += 1;
    }
}
let errorRate = IntAsDouble(differences)/IntAsDouble(Length(eavesdropppingIndices));
Message($"Error rate: {errorRate*IntAsDouble(100)}%");
if (errorRate > 0.1) {
    Message($"Eavesdropper detected! Aborting the protocol");
    Message("");
    return false;
} else {
    Message($"No eavesdropper detected.");
}
```

Finalmente se trunca la clave resultante para quedarnos con una clave de longitud n. En caso de no haber conseguido la longitud suficiente se aborta el protocolo.

```
Message($"Alice's key: {BoolArrayToString(aliceKey)} | key length: {IntAsString(Length(aliceKey))}");
Message($"Bob's key:   {BoolArrayToString(bobKey)} | key length: {IntAsString(Length(bobKey))}");

if (Length(aliceKey) < expectedKeyLength) {
    Message("Key is too short, aborting the protocol");
    return false;
}

let trimmedKey = aliceKey[0..expectedKeyLength-1];
Message($"Final trimmed {expectedKeyLength} bit shared key: {BoolArrayToString(trimmedKey)}");

return true;
```

Para visualizar el protocolo invocamos la operación con los parámetros 256 (indicando la longitud de la clave) y 1 (indicando la posibilidad de que exista un espía).

```
@EntryPoint()
operation Start() : Unit {
    let result2 = RunEPRQKDProtocol(256, 1.0);
    Message("Running the protocol for 256 bit key with eavesdropping probability 1 resulted in " +
(result2 ? "succcess" | "failure"));
}
```

Obtenemos como resultado un error del 19% que por ser superior a la cota aborta el proceso:

```
Running the EPR QKD protocol for expected key length: 256
```

```
Performing eavesdropping check....
Error rate: 19,413919413919416%
Eavesdropper detected! Aborting the protocol

Running the protocol for 256 bit key with eavesdropping probability 1 resulted in failure
```

Si lo ejecutamos suponiendo que no existe un espía:

```
@EntryPoint()
operation Start() : Unit {
    let result2 = RunEPRQKDProtocol(256, 0.0);
    Message("Running the protocol for 256 bit key with eavesdropping probability 1 resulted in " +
(result2 ? "succcess" | "failure"));
}
```

Vemos que el protocolo funciona: el ratio de error es del 0%, por lo que no se detecta a Eve y Alice y Bob obtienen una clave con la longitud suficiente que después es truncada.

```
Running the EPR QKD protocol for expected key length: 256
Performing eavesdropping check....
Error rate: 0%
No eavesdropper detected.

Alice's key:
0011110010001001000110100110000011111111100111010001001110011111111111100101110011100001011100000101100000101110100011011111010001000110111110100100011010110011110010011111100001010111000111010000000110000111010000100011011110100010101101011001011111000110010111000010110100011100000111 | key length: 274

Bob's key:
0011110010001001000110100110000011111111100111010001001110011111111111100101110011100001011100000101100000101110100011011111010001000110111110100100011010110011110010011111100001010111000111010000000110000111010000100011011110100010101101011001011111000110010111000010110100011100000111 | key length: 274

Final trimmed 256 bit shared key:
0011110010001001000110100110000011111111100111010001001110011111111111100101110011100001011100000101100000101110100011011111010001000110111110100100011010110011110010011111100001010111000111010000000110000111010000100011011110100010101101011001011111000110010111000010
0011011110100010101101011001011111100011001011100001011010001110000111

Running the protocol for 256 bit key with eavesdropping probability 0 resulted in success
```

Observamos que por tanto el protocolo E91 es fiable y seguro ante un ataque por parte de Eve durante la generación de pares entrelazados. Ante la presencia de un espía observamos un error entre las claves de Alice y Bob de más del 15%, por lo que bastaría con establecer una cota menor para garantizar seguridad. A pesar de ello, este protocolo requiere de un gran número de pares EPR para su funcionamiento (al menos 4 veces la longitud deseada de la clave) y basa su eficacia en que este entrelazamiento permanezca estable lo que dificulta su puesta en práctica.

5. REFERENCIAS BIBLIOGRÁFICAS Y ENLACES DE INTERÉS

1. Leyvraz, F. (2019). Entrelazamiento, no-localidad y otras particularidades de la mecánica cuántica. https://www.fis.unam.mx/pdfs/Memorias%20Escuela%20de%20Verano%202019.pdf#page=42

2. Varios autores (2021). Quantum Nonlocality. https://en.wikipedia.org/wiki/Quantum_nonlocality#cite_note-ASPECT-1

3. Einstein, A., Podolsky, B., Rosen, N. (1935). Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? https://journals.aps.org/pr/pdf/10.1103/PhysRev.47.777

4. Varios autores (2021). Teorema de Bell. https://es.wikipedia.org/wiki/Teorema_de_Bell

5. Huemer. M. (2020). Quantum nonlocality. https://www.youtube.com/watch?v=ZYAeuGuqtTM

6. Brassard, G., Lutkenhaus, N., Mor, T., & Sanders, B. C. (2000). Limitations on practical quantum cryptography. Physical review letters, 85(6), 1330–1333. https://doi.org/10.1103/PhysRevLett.85.1330

7. Ekert, A. (1997). From quantum-codemaking to quantum code-breaking. *arXiv preprint quant-ph/9703035*.

8. Servicio Azure Quantum y kit de desarrollo de Quantum (QDK). (s. f.). https://docs.microsoft.com/es-es/azure/quantum/install-overview-qdk

9. Devkit-vscode. (s. f.). devkit-vscode. https://marketplace.visualstudio.com/items?itemName=quantum.quantum-devkit-vscode

10. Introduction to quantum computing with Q# – Part 11, EPR Quantum Key Distribution | StrathWeb. A free flowing web tech monologue. (2020). StrathWeb. https://www.strathweb.com/2020/12/introduction-to-quantum-computing-with-q-part-11-epr-quantum-key-distribution/

11. MOOC Crypt4you UPM. (2014). MOOC Crypt4you UPM. http://www.criptored.upm.es/crypt4you/temas/cuantica/leccion2/leccion02.html