Criptografía Cuántica [*]

M. Baig
Grup de Física Teòrica - IFAE
Facultat de Ciències, Ed. Cn
Universitat Autònoma de Barcelona
08193 Bellaterra (Barcelona)

Resumen

Después de una breve introducción a la criptografía clásica y su relación con la teoría de la información de Shannon se introducen los elementos básicos de la criptografía cuántica y sus realizaciones experimentales. Acompañan al curso dos *notebooks* de Mathematica que implementan los protocolos One-Time-Pad y RSA.

Contenido

[*]Lecturas impartidas en la IX Escuela de Otoño de Física Teórica. Santiago de Compostela. 2001

1. Introducción

Richard Feynman inicia su curso de Mecánica Cuántica con un experimento ideal, basado en la doble rendija de Young, que le permite distinguir entre una situación clásica y una de cuántica. Una máquina lanza partículas (balas o electrones) sobre una pared con una doble rendija, por delante de una pantalla donde impactar.

En un sistema *clásico* las trayectorias de las balas son distinguibles, es decir, se puede seguir el camino que sigue cada una. Los impactos en la pantalla seguirán una distribución estadística, resultado de sumar los impactos individuales de las distribuciones que se obtendrían separando las balas que han pasado por una rendija o por la otra. Se obtiene, pues, una distribución de probabilidad que es la suma de las distribuciones de probabilidad de las dos rendijas.

En un sistema *cuántico* las trayectorias individuales no se pueden seguir. Incluso enviando electrones uno a uno, los impactos en la pantalla dibujaran una distribución que mostrará una figura de interferencia, siempre que los dos agujeros estén abiertos.

Podríamos considerar este dispositivo como un canal de comunicación. Por ejemplo, variando la separación de las rendijas, la distribución de los impactos en la pantalla será distinta. Es fácil imaginar un código de comunicación basado en este efecto. ¿Habrá alguna diferencia entre el caso clásico y el caso cuántico?

Si un espía accediera al canal de comunicación (entre las rendijas y la pantalla) podría fácilmente iluminar el camino de las partículas y deducir la figura sobre la pantalla y, por tanto, descifrar el mensaje. Ahora bien, esto seria cierto *solamente* en el caso clásico. Si se usa la misma técnica de espionaje para una comunicación cuántica, la acción del espía !eliminaria la formación de la figura de interferencia¡.

La imposibilidad de observar un sistema cuántico sin perturbarlo está en la base de la aplicación de los sistemas cuánticos al tratamiento de la información. La criptografía, entendida como el conjunto de técnicas para mantener una comunicación segura entre dos partes, es, por tanto, un campo de aplicación ideal de esta característica de los sistemas cuánticos: observar (espiar) modifica (destruye) el sistema observado. Es como si el espía al leer un documento secreto lo perturbara o incluso destruyera. ¿Es realmente posible implementar un sistema de comunicaciones seguro (inviolable) basándose en sistemas cuánticos? La respuesta es positiva: la mecánica cuántica ha abierto una nueva via en la historia de la criptografía, pero, paradójicamente, también ha puesto en cuestión la seguridad de los métodos criptográficos más utilizados actualmente.

En estas lecturas revisaremos los puntos básicos de la dilatada historia de la criptografía y el criptoanálisis para poder entender el papel que la mecánica cuántica esta jugando en este proceso en continua evolución. Asimismo, veremos las principales implementaciones de sistemas criptográficos basados en la mecánica cuántica, actualmente ya en explotación comercial, y el papel que jugarán los futuros ordenadores cuánticos en la criptografía y el criptoanálisis.

2. Cifras monoalfabéticas

Los orígenes de la criptografía se hunden en las profundidades de la historia. En todas las épocas siempre ha habido necesidad de comunicar información de forma secreta. Los primeros en usar un método de comunicación secreta sistemático fueron los antiguos habitantes de Esparta. No obstante, si una figura histórica se ha asociado a los orígenes de la criptografía esta es Julio César.

2.1. La cifra del César

Según cuenta Suetonio en *Vida de los Césares*, Julio César enviaba los mensajes a sus generales sustituyendo cada letra del alfabeto por la correspondiente tres posiciones más avanzada:

Alfabeto llano	a	b	c	d	e	...	x	y	z
Alfabeto cifrado	D	E	F	G	H	...	A	B	C

Ejemplo:

Texto llano	este es un mensaje cifrado
Texto cifrado	HVXH HV XQ PHQVDMH FLIUDGR

Puede complicarse un poco si se eliminan los espacios entre palabras

Texto llano	esteesunmensajecifrado
Texto cifrado	HVXHHVXQPHQVDMHFLIUDGR

Evidentemente, no hace falta limitarse a avanzar tres letras. Tenemos 26 posibilidades de formar una *cifra del César*.

Esta sencilla cifra nos presenta ya los elementos básicos del proceso de encriptación de un texto:

1. **Cifra**: Método de codificación. En este caso el método es la transposición cíclica de las letras del alfabeto.

2. **Texto llano**: texto del mensaje a codificar. Buscaremos siempre métodos que permitan codificar *cualquier* texto, es decir, que evitaremos considerar las claves que se basan en una serie de palabras previamente concertadas con un significado preacordado entre emisor y receptor. En los ejemplos escribiremos siempre el texto llano con letras minúsculas.

3. **Texto cifrado**: texto del mensaje codificado. Lo escribiremos en letras mayúsculas.

4. **Clave**: En este caso es el número 3, es decir, que se avanza el alfabeto cifrado tres posiciones. Debemos distinguir entre el método de cifrado (cifra o código) y la llave (clave). Para estudiar el criptoanálisis se supone que el espía conoce (o puede deducir) el código, pero desconoce la llave.

Principio de Kerkhoff's (1835-1903): La seguridad de un criptosistema reside en mantener secreta la llave

En el siglo XV Leon Batista Alberti (1404-1472) inventó una máquina de cifrar consistente en dos círculos concéntricos, de distinto diámetro, con el abecedario dispuesto circularmente, uno con el alfabeto plano y el otro con el cifrado. Se gira el círculo interior el número de posiciones que indica la clave y la traducción del texto llano al texto cifrado se realiza directamente. AL mismo tiempo, descifrar el mensaje, es decir, pasar del texto cifrado al texto llano se realiza de forma sencilla leyendo el texto cifrado del círculo interior.

La pregunta surge en seguida: ¿es seguro enviar un mensaje usando la cifra del César?. Para responderla hemos de ponernos en la situación del criptoanalista: conoce el método pero ignora la clave. Dado que hay 26 alfabetos distintos, el criptoanalista puede probarlos todos y ver si con alguno de ellos obtiene un menaje legible.

2.2. Cifra monoalfabética

La cifra del César es un caso particular de cifrado monoalfabético en el que la asignación del alfabeto cifrado al alfabeto llano es una simple trasposición.
Cifra Monoalfabética: Es una aplicación

$$\{a, b, c, ..., z\} \rightarrow \mathbf{P}\{a, b, c, ..., z\}, \tag{1}$$

donde $\mathbf{P}\{a, b, c, ..., z\}$ representa el conjunto de las permutaciones de las 26 letras del alfabeto, lo que da un total de $26! = 4 \times 10^{26}$ posibilidades de cifras distintas.

Evidentemente, la cifra del césar forma parte del conjunto de posibles cifras monoalfabéticas ya que las trasposiciones cíclicas en el conjunto de las letras del alfabeto son unas pocas de las posibles permutaciones. ¿Cómo es posible crear una cifra? Pues hay que establecer un diccionario que nos pase del alfabeto llano al alfabeto cifrado, una cualquiera de las 26! posibilidades.

2.2.1. Cifrado mediante palabra clave

La ventaja de la cifra del César se basa en la simplicidad de la clave, transmitir al receptor un sólo número. Una mejora consiste en usar una palabra clave, por ejemplo "SANTIAGO", y usarla como las primeras letras del alfabeto cifrado, eliminando las letras repetidas y disponiendo a continuación el resto de letras. Así:

Alfabeto llano	a	b	c	d	e	f	g	h	i	j	k	l	...
Alfabeto cifrado	S	A	N	T	I	G	O	B	C	D	E	F	...

Esta asignación de alfabetos constituye la cifra basada en la palabra clave "SANTIAGO", y como es fácil comprobar, no corresponde a ningún caso de cifra del césar. Veamos como se codifica el mensaje del ejemplo anterior:

Texto llano	esteesunmensajecifrado
Texto cifrado	IQRIIQUJHIJQSINCGPSTK

¿Es "seguro"enviar un menaje usando este sistema? Evidentemente, al contrario del caso de la cifra del César un análisis exhaustivo de de todos los 26! distintos alfabetos llevará al fracaso. Por este motivo, las cifras monoalfabéticas se consideraron "seguras"durante muchos siglos. Pero, ¿lo son realmente?

2.3. El criptoanálisis

Al-Kindi (s. XI) encontró un punto débil de la codificación monoalfabética: cada letra del alfabeto se substituye por otra, pero siempre la misma. Dado que el texto llano a codificar se encuentra escrito en un *lenguaje natural*, todas las características el mismo se trasmiten al texto codificado. Por ejemplo, la frecuencia de aparición de las distintas letras es una característica propia de cada lenguaje. Así, en inglés, la letra mas frecuente en un texto es la letra *e* que aparece en promedio un $12,702\,\%$ de las veces. La letra *a* aparece un $8,167\,\%$, la letra *b* un $1,492\,\%$ etc.

A partir de esta observación al-Kindi encontró un método de romper una cifra monoalfabética: Si el texto cifrado es lo suficientemente largo, un análisis de frecuencias de los distintos símbolos comparado con el análisis de frecuencias del lenguaje en que está escrito permite deducir la tabla de conversiones de los dos alfabetos.

> ***Una cifra monoalfabética sobre un lenguaje natural es notablemente insegura.***

El criptoanálisis acababa de nacer.

3. Cifras polialfabéticas

Para evitar que el análisis de frecuencias pueda *romper* una cifra, hay que conseguir que las frecuencias de aparición de los distintos símbolos en el texto cifrado sea lo mas homogénea posible. Esto se consigue en las cifras polialfabéticas.

3.1. La cifra Vigenère

Blaise de Vigenère (1523-1596) publicó en el año 1586 el primer método de cifrado polialfabético. Básicamente de trata de codificar el texto llano con la cifra del César, pero usando un desplazamiento (llave) distinto para cada letra del mensaje. Así, si recordamos la cifra del César con la llave 3 para todo el menaje:

Texto llano	m	e	n	s	a	j	e	c	i	f	r	a	d	o
Llave	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Texto cifrado	P	H	Q	V	D	M	H	F	L	I	U	D	G	R

se puede cambiar ahora por el proceso

Texto llano	m	e	n	s	a	j	e	c	i	f	r	a	d	o
Llave	22	5	14	21	19	22	5	14	21	19	22	5	14	21
Texto cifrado	I	J	B	N	T	F	J	Q	D	Y	N	F	R	J

En este ejemplo diríamos que hemos empleado una cifra Vigenère con la llave 22-5-14-21-19. Podemos comprobar que la letra a del texto llano que aparece dos veces, la primera de codifica en una T y la segunda en una F. La principal característica de la cifra Vigenère es que una misma letra se codifica con símbolos distintos, lo que imposibilita un análisis de frecuencias[1].

Si identificamos las trasposiciones por la letra a que va a parar la letra inicial del alfabeto en lugar de por el número de saltos, entonces la llave puede ser una palabra, en el ejemplo anterior seria *venus*

3.2. Criptoanálisis de la cifra Vigenère

Durante dos siglos la cifra Vigenère fue efectivamente inviolable a todos los intentos de los criptoanalistas, hasta que entró en escena Charles Babagge (1792-1871) quien en 1854 encontró un método para romperla. Desgraciadamente para Babagge, su idea fue redescubierta y publicada unos años mas tarde, en 1863, por Kasinski (1805-1881).

El test de Kasinski, como así lo conocemos hoy día, se basa en la búsqueda de combinaciones de dos o tres letras que se repitan en el texto cifrado. Si la llave se repite, hay una cierta probabilidad de que un grupo de letras del texto llano que aparecen juntas a menudo (por ejemplo "que") se codifique con el mismo fragmento de la llave, lo que implicará una repetición en el texto cifrado.

Texto llano	...	q	u	e	.....	q	u	e	...
Llave	...	x	x	x	.....	x	x	x	...
Texto cifrado	...	X	Y	Z	.....	X	Y	Z	...

El método de criptoanálisis empieza por realizar un estudio estadístico de las distancias entre grupos repetidos. A continuación se descomponen estas distancias en factores primos y entonces se puede inferir que *la longitud de la clave será un múltiplo del factor común entre ellos.*

El siguiente paso lo dio Friedman (1925), al introducir el denominado *índice de coincidencias* o probabilidad de que sacadas dos letras al azar de un texto sean la misma. A partir del texto cifrado podemos calcularlo como

$$I_t = \frac{1}{n(n-1)} \sum_{i=1}^{26} n_i(n_i - 1) \tag{2}$$

donde n es el número de caracteres en el texto y n_i el número de apariciones de la letra número i.

Por otra parte, si sabemos el lenguaje empleado, este valor deberá coincidir con el teórico:

$$I = \sum_{i=1}^{26} p_i^2 \tag{3}$$

donde p_i es la probabilidad de aparición de cada letra, calculado a partir de la tabla de frecuencias del lenguaje.

[1] Dependiendo de la clave algunos símbolos pueden también repetirse, como en el caso de la letra e del texto llano del ejemplo anterior

Si el texto ha sido cifrado con una cifra monoalfabética (y la muestra es suficientemente larga) los dos índices coincidirán. Si se trata de una cifra Vigenère polialfabética, entonces el índice I_t disminuirá, tanto más cuanto más larga sea la palabra clave. En otras palabras, el índice de coincidencias nos da información sobre el grado de uniformización de las frecuencias de las letras.

La estimación sobre la longitud de la palabra clave del índice de coincidencias nos permite elegir cual de los múltiplos del valor obtenido en el test de Kandiski debemos proponer como longitud de la palabra clave empleada en la codificación.

El conocer la longitud de la palabra clave permite romper fácilmente la codificación polialfabética. En efecto, basta estudiar con las técnicas habituales del criptoanálisis monoalfabetico los conjuntos de letras del mensaje que se han codificado con el mismo alfabeto, y habrá tantos conjuntos como letras tenga la palabra clave.

4. Criptografía e información

Un criptosistema o esquema de encriptación es un conjunto formado por $(\mathbf{P}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D})$ donde

$$\begin{cases} \mathbf{P}, & \text{Conjunto de textos llanos;} \\ \mathbf{C}, & \text{Conjunto de textos cifrados;} \\ \mathbf{K}, & \text{Conjunto de claves de encriptación;} \\ \mathbf{E}, & \text{Familia de funciones de encriptación;} \\ \mathbf{D}, & \text{Familia de funciones de desencriptación.} \end{cases}$$

Las funciones de encriptación actúan como

$$E_k : \mathbf{P} \to \mathbf{C}, \forall k \in \mathbf{K} \tag{4}$$

y las de desencriptación como

$$D_k : \mathbf{C} \to \mathbf{P}, \forall k \in \mathbf{K} \tag{5}$$

La condición de que un tal sistema constituya un criptosistema es que se verifique la propiedad

$$\forall e \in \mathbf{K}, \exists d \in \mathbf{K} / D_k(E_e(p) = p, \forall p \in \mathbf{P} \tag{6}$$

Un criptosistema se denomina *simétrico* cuando d y e son iguales. Por el contrario, se denomina *asimétrico* si d y e son diferentes.

4.1. Criptoanálisis

Denominamos *Criptoanálisis* al ataque a un criptosistema. Hay que considerar distintos tipos de criptoanálisis, básicamente

- *Ataque de texto cifrado* El criptoanalista sólo conoce el texto cifrado y se quiere conseguir el texto llano y la clave.

- *Ataque con texto llano conocido* Se conoce el texto llano y el texto cifrado y se quiere determinar la llave.
- *Ataque con texto llano escogido* Se pueden encriptar textos llanos pero se desconoce la clave.

En un criptosistema $(\mathbf{P}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D})$ denotamos por $P_{r_p}(p)$ a la probabilidad de que un texto llano p aparezca en en $\mathbf{P}$. De forma similar, la probabilidad de una clave se denota por $P_{r_k}(k)$. La probabilidad de que un texto llano p aparezca codificado por la clave k es, pues, $P_r(p,k) = P_{r_p}(p).P_{r_k}(k)$, función que define una distribución de probabilidad en el espacio producto $\mathbf{P} \times \mathbf{K}$.

Decimos que un criptosistema es *secreto perfecto* si

$$P_r(p|c) = P_r(p), \forall p \in \mathbf{P}, \forall c \in \mathbf{C} \tag{7}$$

es decir, que la probabilidad de un cierto texto cifrado y la probabilidad de que un texto llano haya sido cifrado son independientes.

Teorema de Shannon Sea $|\mathbf{C}| = |\mathbf{K}|$ y $P_r(p) > 0, \forall p \in \mathbf{P}$. El criptograma será secreto perfecto si y sólo si la distribución de probabilidad en el espacio de llaves es uniforme y si para cualquier texto llano p y texto cifrado c, existe una única llave k con $E_k(p) = c$

5. Cifrado digital simétrico

Gilbert S. Vernam (1890-1960) publicó en 1927 un sistema de cifrado conocido por *one time pad* o cuaderno de uso único. El punto débil de la cifra Vigenère reside en la *repetición* de la palabra clave. Si la palabra clave fuese tan larga como el mensaje, el test de Kandiski no podría funcionar. Ahora bien, si hay una estructura de lenguaje natural en la clave, esta estructura puede causar una debilidad y a pesar de todo abre la posibilidad de descifrado. Vernam se dio cuenta de que la única posibilidad realmente segura era que la clave fuese de la misma longitud del mensaje y totalmente aleatoria. En 1949 Shannon demostró que la cifra Vernam era totalmente segura a condición de que no se usase dos veces la misma clave. De aquí el origen del nombre de çuaderno de uso único", la clave aleatoria debe escribirse en un *libro de claves* y usar una hoja distinta para cada mensaje.

Una versión de la cifra Vernam puede aplicarse a los mensajes por ordenador. Cualquier texto llano al introducirse en un sistema informático se traduce en bits. Usualmente, en este paso se usa la codificación ASCII, en donde se reservan ocho bits para cada carácter del texto (incluidos los espacios en blanco). Un texto llano se representa pues por una cadena de ceros y unos, en bloques de ocho bits. La llave será una secuencia de la misma longitud de ceros y unos aleatorios. El proceso de cifrado es idéntico al de la cifra Vigenère con la salvedad de que ahora el alfabeto tiene solamente dos caracteres. Si en la clave hay un cero no se cambia pero si hay un uno se debe permutar el texto llano para codificarlo. Una forma más cómoda de realizar esta operación es aplicar la denominada XOR, implementada en todos los ordenadores, que se basa en la tabla siguiente:

$$0 \bigoplus 0 = 0 \quad (8)$$
$$0 \bigoplus 1 = 1 \quad (9)$$
$$1 \bigoplus 0 = 1 \quad (10)$$
$$1 \bigoplus 1 = 0 \quad (11)$$
$$(12)$$

Si codificamos una cadena de n-bits con este método: $\mathbf{P} = \mathbf{C} = \mathbf{K} = \{0,1\}^n$ y $D_k = E_k$ siendo la operación $p \to p \bigoplus k$. Así, un texto llano $(a_1, a_2, \ldots a_n)$ más una clave $(k_1, k_2, \ldots k_n)$ da lugar a un texto codificado $(c_1, c_2, \ldots c_n) = (a_1 \bigoplus k_1, a_2 \bigoplus k_2, \ldots a_n \bigoplus k_n)$

Para decodificar el mensaje basta sumar otra vez la *misma clave* al mensaje cifrado, dado que, como se puede comprobar fácilmente

$$(c_1 \bigoplus k_1, c_2 \bigoplus k_2, \ldots c_n \bigoplus k_n) = (a_1 \bigoplus k_1 \bigoplus k_1, a_2 \bigoplus k_2 \bigoplus k_2, \ldots a_n \bigoplus k_n \bigoplus k_n) = (a_1, a_2, \ldots a_n)$$

En el apéndice 1 se incluyen dos *Notebooks* de Mathematica con los que se puede practicar la codificación y decodificación digital simétrica OTP.

6. Bases físicas para una criptografía cuántica

Tal como hemos comentado, el teorema de Shannon nos asegura que el cifrado digital simétrico del apartado anterior es secreto perfecto siempre y cuando se cumplan los dos requisitos

1. La llave ha de ser *aleatoria*
2. La llave debe usarse *sólo una vez*

unos requisitos que no parecen muy difíciles de cumplir. Hay, sin embargo, una tercera dificultad: la llave, tan larga como el mensaje y de un solo uso, ha de estar en posesión tanto del *emisor* como del *receptor*. El principal obstáculo de orden práctico es el de como compartir la clave, dado que si cae ésta en manos de terceros el secreto se perdería. Es en este punto donde la mecánica cuántica hace su aparición aportando métodos *seguros* de distribución de llaves (Quantum Key Distribution).

La seguridad de los mecanismos para QKD reside en las bases físicas de la mecánica cuántica:

1. El teorema de *no cloning* que nos asegura que un estado cuántico $|\Psi\rangle$ no puede ser copiado. Clásicamente un texto puede ser fotocopiado. Un sistema cuántico no puede ser copiado, y, por tanto, espiado. **¡No existe la fotocopiadora cuántica!**
2. Cualquier intento de obtener información sobre un sistema cuántico lleva aparejado una cierta modificación del mismo. **¡No hay información sin alteración!**

3. Las medidas cuánticas son irreversibles. Después de realizar una medida, el sistema colapsa a uno de los estados propios del operador correspondiente a la magnitud que se ha medido, y este proceso es irreversible, es decir, no se puede volver a llevar al sistema a su estado original, el de antes de medir. **¡Un espía siempre dejará trazas!**

Veamos con más detalle estos efectos. Supongamos que queremos distinguir entre dos estados cuánticos $|\Psi\rangle$ y $|\Phi\rangle$ que no sean ortogonales, es decir,

$$|\langle\Phi|\Psi\rangle|^2 \neq 0 \tag{13}$$

El aparato de medida que usaremos para distinguirlos se representará por una *ancilla* $|u\rangle$. El estado global será pues $|\Phi\rangle \bigotimes |u\rangle$ o bien $|\Psi\rangle \bigotimes |u\rangle$.

La evolución del sistema durante la medida conllevará a que la ancilla evolucionará hasta un estado que, si queremos nos sirva para distinguir entre los dos, deberá ser distinto en cada caso: $|u_\Phi\rangle$ o bien $|u_\Psi\rangle$. Pero la evolución es unitaria, lo que implica que si queremos que los estados a medir queden inalterados, será imposible que los estados de la ancilla sean distintos.

7. Protocolos para la generación cuántica de llaves (QKG)

Veremos ahora los protocolos básicos que se han implementado incluso experimentalmente para una crear una llave compartida entre dos personas, Alice Y Bob, que se pueden comunicar mediante un canal cuántico (fibra óptica por ejemplo).

7.1. BB84

Este protocolo fue presentado por Bennett y Brassard en la International Conference on Computers, Bangalore (1984). Consideraremos la implementación que usa fotones polarizados. Recordemos que los fotones se polarizan transversalmente, cosa que se puede indicar por un vector en un plano transversal al movimiento. Si elegimos como base para escribir el vector polarización los vectores polarizados según las direcciones de los ejes X e Y podremos escribir un vector polarización (y al estado cuántico correspondiente) según una dirección arbitraria como

$$|\Psi\rangle = a|\rightarrow\rangle + b|\uparrow\rangle \tag{14}$$

donde hemos denotado los estados de la base como $|\rightarrow\rangle$ y $|\uparrow\rangle$.

No obstante, la elección de esta base es totalmente arbitraria. El mismo estado $|\Psi\rangle$ tiene su representación en otra base como por ejemplo la formada por los estados de polarización según las direcciones $|\nearrow\rangle$ y $|\nwarrow\rangle$

$$|\Psi\rangle = a'|\nearrow\rangle + b'|\nwarrow\rangle \tag{15}$$

Las dos bases, que representamos por base $+$ y base $\times$ están relacionadas por las ecuaciones de cambio de base

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle + |\uparrow\rangle) \quad (16)$$

$$|\nwarrow\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle - |\uparrow\rangle) \quad (17)$$

Por convenio, el bit 0 lo representaremos por el estado $|\rightarrow\rangle$ en la base + o por el estado $|\nearrow$ en la base $\times$. Similarmente, al bit 1 lo asignamos a los estados $|\uparrow\rangle$ o $|\nwarrow\rangle$. El uso simultáneo de ambas bases permitirá asegurar la inviolabilidad de la transmisión.

7.1.1. Implementación

Alice genera dos secuencias de bits aleatorios:

Sec. 1	0	1	1	0	0	1	...
Sec. 2	1	0	0	1	1	1	...

La primera secuencia indica el bit a transmitir y la segunda la base en la que debe preparar el estado que representa el citado bit, usando en convenio de que 0 indica la base + y 1 la base $\times$.

Así, en el ejemplo anterior tendríamos:

Bits	0	1	1	0	0	1	...
Bases	$\times$	+	+	$\times$	$\times$	$\times$	...
Estados	$\|\nearrow\rangle$	$\|\uparrow\rangle$	$\|\uparrow\rangle$	$\|\nearrow\rangle$	$\|\nearrow\rangle$	$\|\nwarrow\rangle$	...

La tercera linea de la tabla anterior indica los estados que debe preparar Alice para irlos enviando secuencialmente a Bob.

Por su parte, Bob debe preparar sus aparatos de medida para analizar los estados (fotones) que le llegarán de Alice. Bob tiene dos opciones para medir cada fotón que le llegue, disponer el aparato de medida según la base + o según la base $\times$. Bob debe generar una serie de bits aleatorios y disponer sus aparatos de acuerdo con el resultado, base + si le sale 0 o base $\times$ si es 1. Por ejemplo, Bob preparará sus aparatos de la forma:

Sec.	1	1	0	0	0	1	...
Bases	$\times$	$\times$	+	+	+	$\times$	...

¿Que resultados medirá Bob? Depende de si recibe un estado preparado según una base y lo lee con los aparatos preparados para la misma base o no. Si las bases coincide, Bob obtendrá el mismo estado que le ha sido enviado. Si lo mide con la base equivocada, el resultado que obtendrá es un elemento de esta base con probabilidad 1/2, siendo, pues, un resultado aleatorio. Continuando el ejemplo anterior

Bits de Alice	0	1	1	0	0	1	...
Bases de Alice	$\times$	+	+	$\times$	$\times$	$\times$	...
Estados de Alice	$\|\nearrow\rangle$	$\|\uparrow\rangle$	$\|\uparrow\rangle$	$\|\nearrow\rangle$	$\|\nearrow\rangle$	$\|\nwarrow\rangle$	...
Bases de Bob	$\times$	$\times$	+	+	+	$\times$	...
Estados de Bob	$\|\nearrow\rangle$	R	$\|\uparrow\rangle$	R	R	$\|\nwarrow\rangle$	...
Bits de Bob	0	-	1	-	-	1	...

Con este proceso, en los casos en que ha habido *coincidencia de bases*, Alice i Bob comparten el mismo bit. En los casos en que no ha habido coincidencia, los bits reconstruidos por Bob son aleatorios. Si encontramos la forma de eliminar de la secuencia de bits de Alice i de la secuencia de Bob los casos de no-coincidencia, Alice i Bob tendrían la misma secuencia de bits aleatorios que podrían usar como *clave aleatoria compartida* para un proceso de encriptación tipo *one time pad*. En nuestro ejemplo compartirían la secuencia $\{0, 1, 1, \ldots\}$

¿Como pueden realizar este proceso de filtro? Pues basta que tanto Alice como Bob hagan públicas las secuencias de bases que han usado para preparar y para medir los estados. Comparando las dos listas tanto Alice como Bob pueden eliminar los resultados que se deben desechar.

La pregunta que surge inmediatamente es si esta comunicación pública pone en entredicho la seguridad del establecimiento de la clave. La respuesta es que no. Mientras ni Alice diga que bit ha codificado ni Bob que resultado ha obtenido, publicar las bases no da ninguna información útil para un eventual espía.

7.1.2. Eavesdropping

¿Como podría un eventual espía (Eva) interferir en este proceso?. Evidentemente, si Alice interfiere el canal de comunicación (la fibra óptica por la que circulan los fotones) lo que no puede hacer es .ªpuntar"los estados de los fotones que pasan por la fibra (lo prohíbe el no-cloning). Ahora bien, Alice si que puede cortar la comunicación midiendo el fotón que llega de Alice y enviando un fotón que ella genere a Bob. ¿Puede detectarse este efecto?

La única forma que tienen Alice y Bob de asegurarse de si hay o no la presencia de Eva es hacer publica, antes incluso de filtrar los resultados, una secuencia de bits emitidos y bits medidos. Es fácil comprobar que la probabilidad de acertar el bit (si no hay Eva presente) es de $3/4$, siendo la probabilidad de fallar de $1/4$. En cambio, si Eva está presente, absorbiendo y emitiendo fotones, la probabilidad de acertar es ahora de $5/8$, o la de fallar de $3/8$. En otras palabras, la presencia de Eva se traduce en un incremento del $50\,\%$ en el número de fallos

7.2. B92

Bennet publicó en 1992 (Phys. Rev. Lett., **68** (1992) 3121) un nuevo protocolo para la generación e intercambio cuántico de claves. Consideramos el mismo sistema anterior pero ahora se escogen como representación de los bits 0 y 1 los estados

Bit	Estado
0	$\vert \rightarrow\rangle \equiv \vert 0\rangle$
1	$\vert \nwarrow\rangle \equiv \vert 1'\rangle$

donde la prima recuerda que se trata del estado correspondiente al bit 1 en la que habíamos llamado base $\times$.

Alice prepara una cadena de bits aleatorios y prepara los estados a enviar de acuerdo con la tabla anterior. Así

Bits	0	1	1	0	0	1	...
Estados	$\vert 0\rangle$	$\vert 1'\rangle$	$\vert 1'\rangle$	$\vert 0\rangle$	$\vert 0\rangle$	$\vert 1'\rangle$	...

Por su parte Bob genera su cadena de bits para elegir las bases en que realiza sus medidas (0 base +, 1 base $\times$), pero en lugar de aplicar una medida de von Neuman, Bob aplica ahora a los estados que recibe los operadores de proyección siguientes: Si su bit es 0 (base +), aplica el proyector $P_{not0} = (1 - |0\rangle\langle 0|)$. En cambio si su bit es 1 (base $\times$), aplica el proyector $P_{not1'} = (1 - |1'\rangle\langle 1'|)$.

El resultado de la aplicación del proyector será cero o uno. ¿Cómo interpretamos los resultados? Si la aplicación de P_{not0} sobre un estado lo deja invariante (autovalor 1), Bob puede estar seguro de que su estado no es $|0\rangle$ y por lo tanto que ha recibido el estado $|1'\rangle$, pero si obtiene cero, no puede deducir que estado ha recibido. De forma similar ocurre con el otro proyector.

La estrategia consiste en eliminar de la secuencia los bits en los que Bob ha medido cero, sea cual sea el proyector que ha aplicado, y quedarse con los que ha medido 1. Una vez realizada la secuencia de medidas, Bob debe comunicar a Alice que bits debe desechar y en los demás el acuerdo será total.

7.3. Protocolo B92 modificado

El protocolo **B92** fue modificado en 1994 por Ekert et al. (Phys. Rev. **A 50** (1994) 1047). La modificación consiste en usar medidas generalizadas (Positive Operator Valued Measurements) (POVM's) en lugar de aplicar directamente proyectores. Así, introducimos los operadores hermíticos y positivos

$$A_0 = \frac{P_{not0}}{1 + \|\langle 0|1'\rangle\|} \tag{18}$$

$$A_{1'} = \frac{P_{not1'}}{1 + \|\langle 0|1'\rangle\|} \tag{19}$$

$$A_? = 1 - A_0 - A_{1'} \tag{20}$$

En conjunto de los tres operadores $\{A_0, A_{1'}, A_?\}$ constituye un POVM

En los tres protocolos anteriores la forma de controlar los errores del canal así como la presencia de Eva consiste en comparar un determinado número de bits de la clave final, estimar la tasa de error y ver si está dentro de los márgenes de los errores estimados. Hay, sin embargo, otros protocolos en los que la presencia de Eva se controla por mecanismos cuánticos, como las desigualdades de Bell. Para ello, estos protocolos usan parejas de estados entrelazados.

7.4. Protocolo E91

Este protocolo presentado en 1991 por Ekert (Phys. Rev. Lett. **67** (1991) 661) usa parejas de fotones entrelazados creados a partir de una fuente EPR (Einstein, Podolski, Rosen). Se consideran tres preparaciones distintas de parejas entrelazadas:

$$|\Omega_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1|\frac{3\pi}{6}\rangle_2 - |\frac{3\pi}{6}\rangle_1|0\rangle_2)$$

$$|\Omega_1\rangle = \frac{1}{\sqrt{2}}(|\frac{\pi}{6}\rangle_1|\frac{4\pi}{6}\rangle_2 - |\frac{4\pi}{6}\rangle_1|\frac{\pi}{6}\rangle_2)$$

$$|\Omega_2\rangle \;=\; \frac{1}{\sqrt{2}}(|\frac{2\pi}{6}\rangle_1|\frac{5\pi}{6}\rangle_2 - |\frac{5\pi}{6}\rangle_1|\frac{2\pi}{6}\rangle_2)$$

donde el valor del ket indica la dirección del eje de polarización de cada fotón.

Para la codificación de consideran tres alfabetos alternativos, que denominamos A_0, A_1 y A_2, con la representación de los bits (0,1) como

Bits	0	1
A_0	$\|0\rangle$	$\|\frac{3\pi}{6}\rangle$
A_1	$\|\frac{\pi}{6}\rangle$	$\|\frac{4\pi}{6}\rangle$
A_2	$\|\frac{2\pi}{6}\rangle$	$\|\frac{5\pi}{6}\rangle$

Como operadores de medida pueden escoger entre $M_0 = |0\rangle\langle 0|$, $M_1 = |\frac{\pi}{6}\rangle\langle\frac{\pi}{6}|$ y $M_2 = |\frac{2\pi}{6}\rangle\langle\frac{2\pi}{6}|$.

El protocolo sigue los siguientes pasos:

1. Se genera un estado $|\Omega_j\rangle$ con $j = 1, 2, 3$ de forma aleatoria.
2. Se manda uno de los fotones a Alice y el otro a Bob
3. Alice y Bob separadamente y de forma aleatoria eligen uno de los tres operadores de medida y lo aplican a su fotón.
4. Después de las medidas, Alice y Bob hacen públicas las listas con los operadores que han usado en cada medida (manteniendo reservados los resultados obtenidos).
5. En los casos en que los dos han usado *el mismo* operador, tienen asegurada la concordancia de los bits medidos. Rechazan todos los demás bits y se quedan con la clave común.

8. Realizaciones experimentales de Criptografía Cuántica

La distribución cuántica de llaves (QKG) es ya una realidad. Diversos grupos experimentales han realizado experimentos de generación de llaves y cifrado de mensajes usando estas llaves. Presentamos a continuación unos de los primeros experimentos publicados.

8.1. Underwater quantum coding

En el articulo de Muller, Zbinder y Gisin (Nature, **378** (1995) 449) podemos leer:

> "Here we report a cryptographic channel using a 23km optical cable below the lake Geneva. A 1.300nm pulsed laser with 1ns pulse width and 1.1MHz pulse rate was used. The key was encoded using the polarization of light pulses manually selected by a rotating polarizer placed after $\lambda/4$ wave plate. A polarization controller, compensating the polarization modification due to the fiber link, was used to align the emission and measurement axis."

En sus conclusiones afirman haber demostrado la posibilidad de realizar sistemas criptográficos cuánticos usando polarización en láseres de 1300nm sobre fibra óptica. El error observado (una tasa del 3,4 %) lo consideran suficientemente bajo como para garantizar la privacidad del canal de comunicación.

8.2. Quantum Cryptography with Entangled Photons

Jennewein, Simon, Wheihs, Weinfurter y Zeilinger (Phys. Rev. Lett.) presentan una completa implementación de la criptografía cuántica con dos usuarios, separados e independientes uno del otro en términos de la localidad e Einstein y explotando las características de los pares de fotones entrelazados. Su implementación se basa en una modificación del protocolo BB84 presentada por Bennet, Brassard y Mermin (Phys. Rev. Lett. **68** (1992) 557) en la que se usan pares de fotones entrelazados. De esta forma evitan el problema de usar pulsos de laser atenuados que tienen una probabilidad no nula de contener más de un fotón, caso susceptible de ser atacado mediante una técnica de "beam splitter".

Los fotones de una fuente EPR y polarizados adecuadamente se transmiten por fibra óptica a Alice i Bob, separados en el experimento citado unos 360m, y ambos fotones son analizados, detectados y registrados independientemente.

Como ejemplo de transmisión de un mensaje usando la llave comunicada por el canal cuántico realizaron la transmisión de una imagen digitalizada de la *venus de Willendorf* formada por 49.984 bits. El sistema es capaz de generar llaves a un ritmo de 400-800 bits/segundo con errores del 3 %

9. Cifrado digital asimétrico

Los sistemas criptográficos vistos hasta ahora tienen la propiedad de que si alguien puede codificar un mensaje también puede decodificarlo, dado que la llave le permite ambas acciones. Los protocolos *asimétricos* explotan un punto de vista distinto en el cual la llaves de cifrar y descifrar son distintas. Estos protocolos se introdujeron en 1976 a raíz de los trabajos de W. Duffie y M. Hellmann y pretenden eliminar el difícil problema de la distribución de claves (clásica o cuántica).

Dado un mensaje p en los sistemas asimétricos existen dos funciones distintas E_p para codificarlo y D_p para decodificarlo. La clave de cifrar se hace *pública* para que cualquiera pueda encriptar un mensaje y enviarlo al receptor. La clave de descifrado se mantiene *privada* para que únicamente el receptor pueda decodificar los mensajes. Este método requiere, pues, la generación de un juego de dos llaves, una que se hace pública y la otra que se mantiene privada. Además, es imprescindible que a partir de la llave pública sea *imposible* deducir la llave privada.

Si Alice quiere enviar un menaje a Bob le basta buscar la llave pública de Bob (E_B), cifrar su mensaje (m) con ella $E_B(m)$ y enviarselo a Bob. A su recepción, Bob aplica su clave privada $D_B(E_B(m)) = m$ y recupera el mensaje. Cualquier interceptación del mensaje enviado es inútil si no se conoce la clave privada.

La estructura matemática de estas funciones de cifrado abre la puerta a una nueva aplicación de la criptografía, la firma de mensajes. Dado que se verifica también que

$E_B(D_B(m) = m$, se puede realizar la siguiente estrategia: Alice cifra un mensaje de confirmación m con su propia llave privada D_A y lo añade al mensaje que quiere enviar. Si Bob quiere estar seguro de que el mensaje recibido procede efectivamente de Alice, le basta buscar la llave publica de Alice y aplicarla al mensaje de confirmación: $E_A(D_A(m)) = m$. Si el resultado es legible, entonces esto garantiza que el texto de confirmación se encriptó con la llave privada de Alice y, por tanto, que efectivamente fue Alice quién escribió en mensaje.

Los sistemas asimétricos han de basarse en encontrar una pareja de funciones de encriptación/desencriptación que muestren una dificultad diferente de realización. Por ejemplo, es fácil dados dos números primos p y q multiplicarlos y obtener un número $n = p \times q$. No obstante, el proceso inverso, es decir, dado n encontrar sus factores primos p y q es mucho mas difícil. En esta dificultad reside la seguridad de los sistemas de llave pública. Como veremos más adelante, estos sistemas no muestran un secreto perfecto, en el sentido de Shannon sino que su seguridad es meramente *computacional*. Si el tiempo (y recursos) que hay que invertir para deducir la llave privada a partir de la pública es lo suficientemente *grande*, el sistema es a la práctica *seguro*.

9.1. RSA

En 1977 Ronald Rivest, Adi Shamir y Leonard Adleman crearon el denominado sistema RSA de criptografía de clave pública, uno de los más populares hoy en día por su uso en Internet.

Para crear un juego de llaves (pública/privada) Bob busca dos números primos *grandes* p y q, y calcula $n = p \times q$. Al mismo tiempo busca dos enteros d y e de tal manera que se verifique que

- d sea *coprimo* con $(p-1) \times (q-1)$
- e sea inverso modular de d (Es decir, solución de $e \times d \equiv 1 \bmod (p-1) \times (q-1)$)

Realizado este proceso, Bob tiene ya el juego de llaves público y privado:

- La llave pública de Bob es el conjunto de números $\{e, n\}$
- La llave privada de Bob es el conjunto de números $\{d, n\}$

9.1.1. Encriptación de un mensaje

Si Alice quiere enviar un mensaje M a Bob, primero debe convertir el mensaje en un número (o una serie de números) decimales. Una forma sencilla de realizar esto es la siguiente

$$M_{texto} \longrightarrow M_{ASCII} \longrightarrow M_{binary} \longrightarrow M_{decimal} \tag{21}$$

Si el texto es largo, resulta conveniente cortar el mensaje decimal en bloques de un cierto número de dígitos y codificarlos por separado.

Dado un bloque numérico M del mensaje de Alice, y conocida la clave pública de Bob e, n, el proceso de encriptación es

$$E = M^e mod(n) \tag{22}$$

El número E representa el mensaje encriptado.

9.1.2. Desencriptación de un mensaje

Cuando Bob recibe el mensaje encriptado E busca su clave privada y realiza la operación:

$$M = E^d mod(n) \tag{23}$$

con lo que recupera el mensaje numérico desencriptado. Invirtiendo el proceso de traducción a números

$$M_{decimal} \longrightarrow M_{binary} \longrightarrow M_{ascii} \longrightarrow M_{texto} \tag{24}$$

se recupera el mensaje de texto.

En el segundo apéndice se incluyen tres *Notebooks* de Mathematica uno para generar las claves, otro para encriptar y un tercero para desencriptar textos aplicando el método RSA.

9.1.3. Seguridad en RSA

La seguridad de RSA reside en la dificultad de encontrar la clave privada a partir de la pública, cosa que se lograría si se pudiera factorizar n (público) en sus factores primos. Hasta ahora, el método más eficiente de factorizar grandes números (el algoritmo de Euclides) necesita un tiempo de cómputo que aumenta exponencialmente con el número de dígitos de n. Es, pues, un problema de la clase NP, aunque no se haya demostrado de forma rigurosa. RSA es *computacionalmente seguro*

Si se descubriese un método de factorización que necesitase un tiempo que aumentase de forma polinómica con el número de dígitos de n, la seguridad de RSA seria puesta en entredicho.

Peter Shor ha demostrado que en un ordenador cuántico se puede implementar un algoritmo de factorización *polinómico*. El algoritmo de Shor, pues, marca el final de la seguridad RSA (siempre y cuando tengamos un ordenador cuántico a nuestra disposición).

10. Bibliografia

1. Simon Singh. "Los códigos secretos". Ed. Debate. (Libro de divulgación sobre la historia de la criptografia)

2. Albretcht Beutelspacher. Çriptology". Mathematical Association of America. (Manual de criptografía clásica)

3. Josef Gruska. "Quantum Computing". McGraw Hill. (Dedica el capítulo 6 a la criptografía cuántica)

4. Michael A. Nielsen and Isaac L. Chuang. "Quantum Computation and Quantum Information". Cambridge University Press (Cap. 12.6)

5. Hoi-Knong Lo. "Quantum Criptology"en "Introduction to Quantum Computation and Information", Ed. by Lo, Popescu and Spiller. World Scientific.