EL EXTRAÑO Y PRODIGIOSO MUNDO DE LOS QUANTA [1]

ALBERTO GALINDO
Real Academia de Ciencias

UN RECUERDO OBLIGADO

El 14 de diciembre del año 2000 se cumple el centenario de uno de los momentos más gloriosos de la física. Max Planck (figura 1) presentaba ante la Sociedad Alemana de Física su famoso trabajo [2] donde, en «un acto de desesperación», discretizaba los cambios de energía de un oscilador e introducía en la física la constante universal h. La palabra *quantum* y su plural *quanta* para denominar a las unidades discretas de acción y energía aparecerían varios años más tarde. Otro genio de la época, Albert Einstein (figura1), en su *annus mirabilis* de 1905, explicaría el efecto fotoeléctrico postulando [3] que la energía de la luz monocromática de frecuencia ν está concentrada en forma de gránulos indivisibles de valor $h\nu$. Estos quanta de luz recibirían veinte años después el nombre de fotones [4].

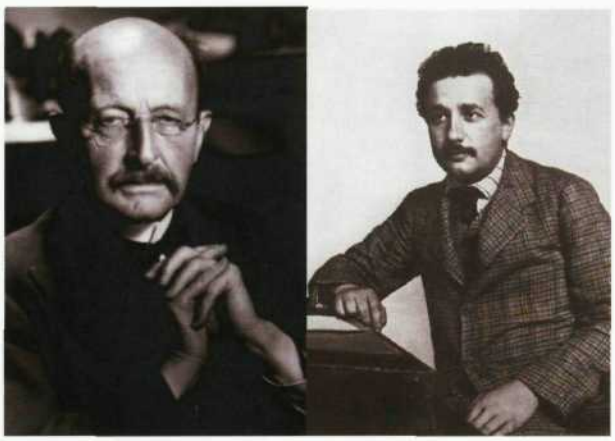

Fig. 1.– Izquierda, M. Planck (1858-1947). Derecha, A. Einstein (1879-1955).

La caja de Pandora estaba abierta. Nunca más sería nuestra visión de la realidad igual que antaño. El encanto de la discretización andaba ya suelto, y pronto asomaría doquiera: en los fotones, en el átomo de hidrógeno *à la* Bohr (1913), etc. El quantum por antonomasia es el fotón; pero el sufijo *ón* acompaña ya a numerosas entidades físicas que aparecen como partes elementales o cuantos de algo: fonón, fluxón, excitón, rotón, etc. Y el hecho profundo de que sean iguales entre sí, diferentes aunque indistinguibles, todos los electrones del Universo, o todos los protones, etcétera, es simple consecuencia de ser los quanta de un único campo cuántico, el del electrón en un caso, el del protón en otro, etcétera.

En el primer cuarto del siglo nueve genios sentaron las bases físicas y conceptuales de la nueva física: Planck (1900), Einstein (1905) y Bohr (1913), seguidos de De Broglie (1923), Heisenberg (1924), Pauli (1925), Schrödinger (1926), Born (1926) y Dirac (1928). El clásico libro de Dirac *(The Principles of Quantum Mechanics)* resume, como ningún otro, las extraordinarias creaciones de estos titanes.

En esta charla trataré de presentar, en lenguaje llano, algunas muestras del comportamiento insólito de los quanta, así como de las repercusiones de la física cuántica en el campo de la información. Pero antes, añadiré unas palabras acerca de los éxitos sin par de la física de los quanta y de su extraordinaria precisión.

---

[1] Conferencia en Logroño (Casa de las Ciencias, diciembre 9), Cuenca (Centro Cultural Aguirre, 20 enero 2000), y Segovia (Torreón de Lozoya,1 de febrero 2000, y Academia de Artillería, 8 de febrero 2000), dentro del Programa de Promoción de la Cultura Científica II organizado por la Real Academia de Ciencias y las Fundaciones BBV y Ramón Areces.

[2] Título del trabajo: «Zur Theorie der Gesetzes der Energieverteilung im Normalspektrum» (Sobre la teoría de la ley de distribución de energía del espectro normal), *Verhandlungen der Deutschen Physikalischen Gesellschaft*, 2, págs. 237-245, 1900.

[3] Título del trabajo: «Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt» (Sobre un punto de vista heurístico concerniente a la producción y transformación de la luz), *Annalen der Physik*, 17, págs. 132-148, 1905.

[4] El químico G. N. Lewis publicó en 1926 un artículo titulado «The Conservation of Photons» en el que propone un mecanismo de enlace químico basado en unas partículas que llamó *fotones*. El nombre cuajó, aunque, evidentemente, no el significado por él propuesto.

ÉXITOS DE LA FÍSICA CUÁNTICA

El impacto de esta naturaleza discontinua ha sido tremendo. El espectro discreto de energías de un sistema físico lo identifica generalmente, y gracias a eso hemos podido conocer, por ejemplo, la composición química de las estrellas, y la expansión del Universo. La microfísica actual, desde la escala subnuclear hasta la molecular, sería inconcebible sin el auxilio de los principios cuánticos. La física de la materia condensada, en la que se apoya básicamente gran parte de la tecnología que nos rodea, cambió dramáticamente con la mecánica cuántica (MQ). Los fenómenos más espectaculares de la materia, como la superconductividad y superfluidez, son consecuencia de cuasicondensaciones cuánticas Bose-Einstein. La miniaturización creciente (nanotecnología, sistemas mesoscópicos) ha hecho posible experimentar el efecto de la dimensionalidad, revelando las espectaculares diferencias entre los comportamientos de los sistemas 0D (motas o puntos cuánticos), 1D (hilos o alambres cuánticos), 2D (gases bidimensionales) y 3D (sistemas ordinarios). Incluso en la evolución del Universo es necesario invocar la MQ para describir los procesos elementales que ocurrieron hasta la liberación de la luz y mucho más tarde en la producción de energía en las estrellas, y para adentrarnos en la época de Planck, los primeros 10^{-43} s tras la Gran Explosión. Basta hojear el número de marzo 1999 de *Reviews of Modern Physics,* celebrando el centenario de la American Physical Society, y que empieza con un artículo de Hans Bethe sobre Quantum Mechanics, para ver la MQ en todos los rincones de la física, incluida por supuesto la Física Biológica.

Precisión de la MQ

El acuerdo entre teoría basada en MQ y experimento ha alcanzado las más altas cotas conocidas en la física. Un par de ejemplos bastan: 1) En el problema típico de 3 cuerpos dado por el átomo bielectrónico de He, el cálculo teórico, una vez incluidas las correcciones pertinentes tanto de masa, como relativistas y radiativas o de electrodinámica cuántica (EDQ), las energías de ionización de algunos estados excitados (como el $1s2s\,^1S_0$) concuerdan con los valores exprimentales con precisión de 1 parte en 10^9. 2) Lo mismo ocurre con el momento magnético anómalo del electrón, expresado a través de su anomalía $a_e := \frac{1}{2}(g_e - 2)$, cuya predicción teórica mediante la EDQ ajusta el valor observado en precisión similar a la anterior[5].

LA SORPRENDENTE FÍSICA DE LOS QUANTA

Si cierto es que la relatividad de Einstein demolió creencias tan arraigadas como la existencia del espacio y del tiempo con carácter absoluto, o la simultaneidad, desde el punto de vista epistémico ha sido seguramente más perturbadora la teoría de los quanta de Planck que ha dado origen a la actual física cuántica. Con ella se ha derrumbado el determinismo laplaciano, las leyes del azar se han enseñoreado de la predicción científica, lo continuo y lo discreto han dejado de ser antagónicos para convivir en armoniosa dualidad, y media realidad se oculta para dejar ver a la otra mitad.

Características de la física cuántica son[6]:

1. la indefinición objetiva,
2. el azar y probabilidad objetivos,
3. el enredo.

La indefinición

Significa que en un estado cuántico α, aunque esté máximamente conocido, hay siempre eventualidades E (proposiciones sí/no) indefinidas, que no son ni ciertas ni falsas. Cuando se somete a consulta al sistema en estado α para ver si una cierta eventualidad E, (por ejemplo, estar en una cierta región), es cierta o no, el resultado es objetivamente azaroso, con unas probabilidades que dependen sólo del estado α y de la eventualidad E, y no del ánimo o conocimientos del experimentador. Decimos que la eventualidad E es potencial en α (no tiene un valor definido) y que la acción de una de estas consultas (medida de E) actualiza su potencialidad.

Un estado cuántico es, por así decirlo, una red de potencialidades; consta no sólo de aquellas eventualidades que tiene bien definidas (hablamos entonces de propiedades del estado), sino también de las probabilidades de hallar cierto o falso al actualizar las otras eventualidades, las indefinidas.

El azar cuántico

En el mundo cuántico manda la ventura, y para describir sus fenómenos recurrimos a las probabilidades. Pero no es un mundo azaroso alocado, sino sometido a una reglas muy precisas. La probabilidad $P(\beta,\alpha)$ de que en un estado α del sistema hallemos como ciertas unas eventualidades que, de estar bien definidas, harían que el sistema estuviese en un estado β, viene dada por $|(\beta,\alpha)|^2$, donde la amplitud de probabilidad (β,α) es un número complejo.

El lenguaje de la nueva física es el lenguaje de las amplitudes de probabilidad, con las que, como acabamos de decir, se predice la probabilidad de que algo ocurra en el mundo físico; las certezas se han evaporado, y por mucho que afinemos en el conocimiento del estado inicial de un sistema físico subsisten elementos de ignorancia irreductibles.

---

[5] Más detalles en A. Galindo, *Revista Española de Física,* 14 (número especial: *Cien años de quanta),* págs. 1-3, 2000.

[6] Véase el artículo de Abner Shimony en *The New Physics.*

Pero estas probabilidades cuánticas obedecen a unas reglas de juego muy peculiares e inequívocas: cuando algo puede ocurrir de varias maneras indistinguibles, la probabilidad de que ocurra no es la suma de las probabilidades individuales (como ocurre al tirar un dado), sino el cuadrado de la suma de sus «raíces cuadradas», de sus amplitudes de probabilidad. Y como las raíces cuadradas pueden ser positivas y negativas (mejor dicho, tienen fase), puede muy bien ocurrir que se cancelen y que la probabilidad total sea nula (interferencia destructiva). ¿Alguien esperaría que al arrojar a la vez dos dados no trucados nunca pudieran sumar 3, cuando lo común sería que esa suma se diera una vez cada 18, en promedio? Pues eso podría ocurrir con dados cuánticos.

Cuando las potencialidades no se actualizan, esto es, cuando las alternativas son indistinguibles, las amplitudes se suman antes de calcular la probabilidad: por ejemplo,

$$(\beta,\alpha)=\sum_{\gamma}(\beta,\gamma)(\gamma,\alpha),\quad P(\beta,\alpha)=|\sum_{\gamma}(\beta,\gamma)(\gamma,\alpha)|^2$$

donde γ es un estado cualquiera con propiedades definidas para un conjunto completo de eventualidades compatibles (es decir, simultáneamente medibles) no actualizadas. Pero si éstas se observan, la probabilidad pasa a valer

$$\overline{P}(\beta,\alpha)=\sum_{\gamma}|(\beta,\gamma)|^2|(\gamma,\alpha)|^2=\sum_{\gamma}P(\beta,\gamma)P(\gamma,\alpha)$$

Decimos entonces que al medir se rompe la coherencia de las diferentes alternativas.

Estas reglas explican una de las peculiaridades de los quanta, su disposición a interferir. No es lo mismo el cuadrado de la suma que la suma de cuadrados:

$$|(\beta,\alpha)|^2=|\sum_{\gamma}(\beta,\gamma)(\gamma,\alpha)|^2\neq\sum_{\gamma}|(\beta,\gamma)(\gamma,\alpha)|^2$$

En la primera igualdad se producen interferencias cuánticas, pues las alternativas γ no se materializan. La desigualdad corresponde al caso de que se actualicen estas eventualidades.

Luz: clásica vs *cuántica*

La polarización de la luz nos ofrece un ejemplo ilustrativo de la diferencia entre los comportamientos clásico y cuántico de la radiación electromagnética[7]. Tenemos un haz de luz no polarizada, y disponemos de 3 polarizadores (Vertical, Diagonal y Horizontal). Al intercalar el *V*, el haz transmitido se atenúa justo a la mitad (figura 2). Si realmente el polarizador fuese una criba clásica, sólo debería dejar pasar los fotones verticalmente polarizados, que son muy pocos en un haz en que todas las polarizaciones son posibles, y la intensidad transmitida sería inapreciable. No es así. Si a continuación ponemos el polarizador *H* en el haz transmitido por el *V*, se bloquea el paso a los fotones, y no pasa nada de luz. Todo pasa ahora como si el polarizador actuara de criba. Pero si finalmente intercalamos entre el *V* y el *H* el polarizador diagonal *D*, de nuevo vuelve a pasar luz tras el *H* (justo 1/8 de la intensidad inicial), contra toda intuición clásica, que nos induciría a pensar que la presencia del nuevo filtro *D* nunca debería ayudar a pasar luz, sino todo lo contrario.

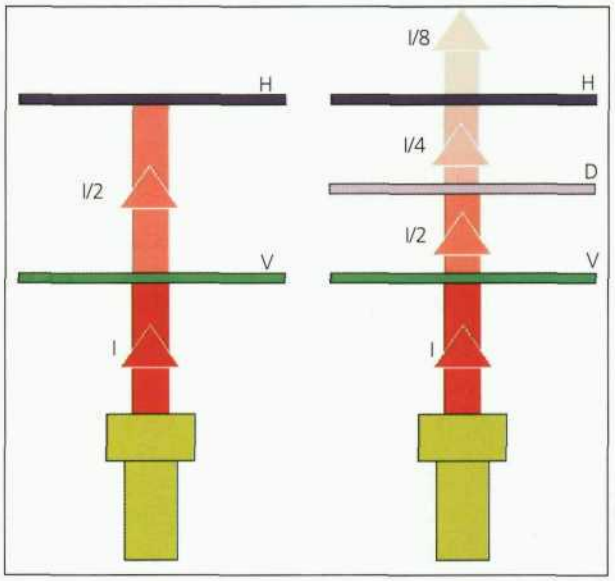

Fig. 2.– Intensidades de un haz tras atravesar polarizadores interpuestos *V*, *H* y *D*.

¿Cómo se explica este sorprendente comportamiento? Cada fotón de vector de polarización ε tiene una cierta probabilidad de atravesar un polarizador *P* que viene dada por $|\varepsilon\cdot\pi_P|^2$, módulo al cuadrado de la amplitud de probabilidad que en este caso es simplemente el producto escalar de ε y del vector unidad π_P a lo largo del eje del polarizador. En el primer caso (fotones no polarizados), esa probabilidad de transmisión $|\varepsilon\cdot\pi_V|^2$ hay que promediarla sobre todas las direcciones ε transversales al momento del haz; resultado, 1/2. En el segundo caso, una vez que el fotón ha conseguido pasar el polarizador *V*, y por tanto tiene un vector polarización π_V, la probabilidad de su transmisión por *H* es $|\pi_V\cdot\pi_H|^2=0$, y no pasa la luz. Y en el tercer caso, la probabilidad de transmisión de la terna *V, D, H* es

$$|\varepsilon\cdot\pi_V|^2\,|\pi_V\cdot\pi_D|^2|\pi_D\cdot\pi_H|^2=$$
$$|\varepsilon\cdot\pi_V|^2\,(1\sqrt{2})^2(1\sqrt{2})^2$$

que tras promediar sobre ε, da 1/8.

Doble rendija

En el volumen III de *The Feynman Lectures in Physics* (1965) se lee que el familiar experimento de la doble rendija *has in it the heart of quantum mechanics. In reality, it*

[7] Véase E. G. Rieffel y W. Pollack, en http://xxx.unizar.es/archive/quant-ph/9809016, así como A. Shimony, *loc. cit.*

contains the only mistery. Se refería Feynman con ello al principio de superposición lineal para estados de una partícula. Cuando un quantum va de un punto a otro puede generalmente hacerlo a lo largo de muchos caminos Γ distintos e indistinguibles, y cada una de estas alternativas interviene con una amplitud compleja de probabilidad α_Γ, de modo que la amplitud total α de llegar a la meta es $\Sigma_\Gamma \alpha_\Gamma$, y la probabilidad asociada $P = |\Sigma_\Gamma \alpha_\Gamma|^2$. Si las amplitudes tienen fases similares, P será mayor que $\Sigma_\Gamma P_\Gamma$, y decimos que la interferencia ha sido constructiva. Pero si hay amplitudes con fases opuestas, puede ocurrir que P sea menor que $\Sigma_\Gamma P_\Gamma$, e incluso nula, y la interferencia habrá sido destructiva. En cambio, si se sabe el camino seguido, o si éste queda registrado en algún sitio, o si en principio podríamos saberlo si quisiéramos, se dice que las alternativas son (físicamente) distinguibles, y $P = \Sigma_\Gamma P_\Gamma$.

Una fuente muy débil emite partículas (de una en una, muy distanciadas en el tiempo) frente a una doble rendija. Si no podemos saber a través de qué rendija pasa cada partícula, la amplitud de probabilidad $\alpha_{12}(X)$ de que una de ellas llegue a un punto X de la pantalla es suma de las amplitudes $\alpha_1(X)$ y $\alpha_2(X)$ de que llegue a través de las rendijas 1 y 2, y la probabilidad

$$P_{12}(X) = \alpha_1(X) + \alpha_2(X)|^2 = P_1(X) + P_2(X) + 2(P_1(X)P_2(X))^{1/2} \cos\phi(X) \neq P_1(X) + P_2(X),$$

donde $\phi(X)$ es la fase relativa entre $\alpha_1(X)$ y $\alpha_2(X)$, mostrará la imagen de interferencias (figura 3).

Pero si nuestra fuente emite pares de partículas «enredadas» con momentos opuestos, de las que una pasa la doble rendija, las interferencias desaparecen, pues la otra partícula del par permite conocer, midiendo su momento, por cuál de las rendijas cruzó su compañera. Y esto ocurre aunque no hagamos esa medida. Basta con su posibilidad para que la interferencia desaparezca (figura 4) [8].

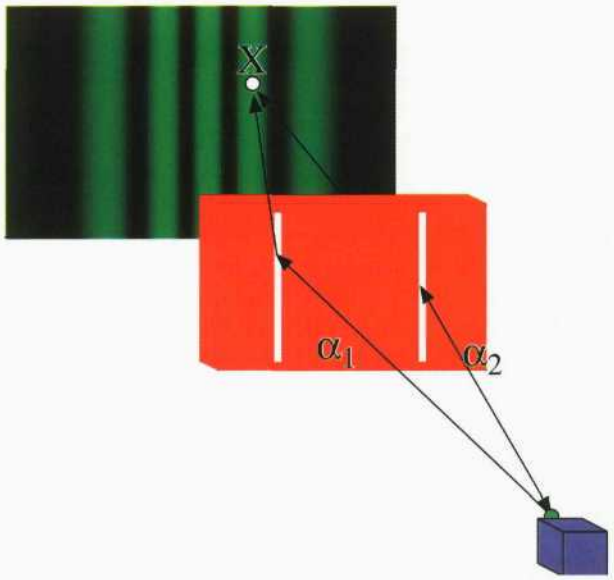

Fig. 3.– Interferencias en doble rendija. La fuente emite partículas que llegan a la pantalla tras atravesar alguna de las dos rendijas. Las amplitudes asociadas se suman antes de calcular la probabilidad de llegar al punto X de la pantalla.

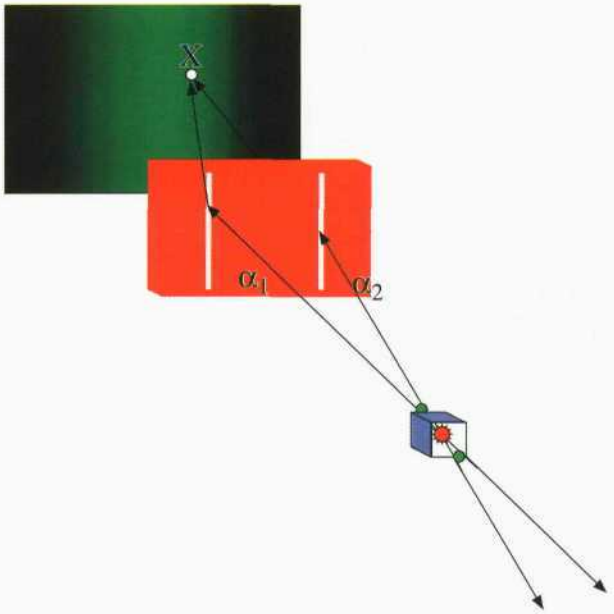

Fig. 4.– *En este experimento intervienen 2 partículas. Una pasa por* las rendijas. La otra, de momento opuesto, permite en principio, midiendo éste, saber por cuál de las rendijas fue la primera, y por tanto, no hay interferencias.

Dualidad onda-partícula

Newton propuso la naturaleza corpuscular de la luz, pero Huygens (1678) defendió su naturaleza ondulatoria, que Young (1801) demostraría brillantemente muchos años después. Al comenzar el siglo XX nadie dudaba de que la luz era una onda electromagnética (EM). Pero ciertos fenómenos (como el efecto fotoeléctrico, y el efecto Compton) requerían la vuelta atrás hacia una imagen de la luz como un chorro de partículas, los fotones. ¿Cómo reconciliar estos aspectos corpusculares con los aspectos ondulatorios, evidenciados por todas las experiencias de interferencia y difracción?

No ha sido fácil aprender a convivir con una realidad extraña que se comporta de dos modos opuestos según el entorno. Nuestro lenguaje ha debido acomodarse; no es «científicamente correcto» decir que la luz es una onda, ni tampoco que es una colección de partículas. No es ninguna de esas cosas, sino ambas a la vez. Dependiendo de las circunstancias externas, se realza una faceta y se deprime la complementaria.

[8] Véase el artículo de Anton Zeilinger en *Reviews of Modern Physics*, marzo 1999.

Corrientemente el aspecto corpuscular de la luz no es discernible debido al elevado número de fotones que hay en una onda EM ordinaria. Pensemos que, por ejemplo, una humilde vela de 0.1 mW en visible arroja por segundo la friolera de 3×10^{14} fotones de esa parte del espectro; a 100 m de distancia el número de tales fotones que penetran en cada uno de nuestros ojos es 10^5. De una estrella de primera magnitud recibimos una energía visual de unos 2×10^{-8} W/m^2, que corresponde a 10^6 fotones por pupila y segundo.

Si las ondas por antonomasia, las ondas EM, se comportan a veces como partículas (de masa nula), ¿no podrán acaso presentarse en ocasiones las partículas (de masa no nula) como si fueran ondas? Esta es la pregunta que se planteó el joven De Broglie (1923-1925) y para la que, por puras consideraciones de analogía y simetría, se atrevió a proponer una respuesta afirmativa, contra toda evidencia secular. Su idea impresionó a Einstein.

De Broglie postuló que toda partícula material lleva asociada una onda «de materia» que la dirige o guía (onda «piloto») en su movimiento; más adelante (Born 1926) se concluiría que se trataba en realidad de una onda amplitud de probabilidad, cuyo módulo cuadrado en un punto era proporcional a la probabilidad de hallar allí la partícula. Si la partícula, de masa m, tiene energía total $E = \gamma(v)mc^2$ y momento lineal $p = \gamma(v)mv$, la onda asociada tiene frecuencia y longitud de onda dadas por las mismas expresiones que rigen para los fotones:

$$\nu = E / h, \quad \lambda = h / p$$

Se conocen como relaciones de Einstein-De Broglie. La segunda proporciona el valor de la longitud de onda de De Broglie.

Los experimentos de Davisson-Germer y de Thomson confirmaron plenamente la existencia de las ondas de materia.

En la vida ordinaria no percibimos esta dualidad: la longitud de onda de los cuerpos macroscópicos es tan pequeña que no hay «ranuras» ni «orificios» que puedan utilizarse para desvelar su aspecto ondulatorio [9]. Sin embargo, ahí está [10].

Ondas de materia

En un bonito experimento [11] se han detectado las ondas de materia asociadas a fullerenos C_{60}. Son los proyectiles de mayor masa (en un orden de magnitud, pues su masa es de unas 720 μam) y complejidad (60 núcleos y 360 electrones, y por tanto con muchos grados de libertad internos excitados) con que se han podido ver interferencias en un experimento del tipo doble rendija (en este caso una red de difracción); hasta la fecha, se habían observado con electrones, neutrones, átomos, dímeros, y cúmulos pequeños de varios átomos de gases nobles ligados por fuerzas de Van der Waals. Los fullerenos fueron producidos en un horno de unos 900-1000 K, que tras pasar por dos ranuras de colimación de 10 μm separadas en 1,04 m, incidían sobre una red de difracción de rendijas de 50 nm y período de separación de 100 nm. La imagen de interferencia se observó a 1,25 m de la red, detectando los fullerenos tras su ionización mediante un rayo láser.

Este experimento revela la interferencia de cada fullereno consigo mismo. Esta interferencia es visible porque no se tiene información de qué camino ha seguido el fullereno. Si éste emitiese luz que nos indicase por qué rendija ha pasado, la imagen de interferencia desaparecería. Para ello es preciso que la longitud de onda λ de la radiación emitida satisfaga $\lambda << d$, siendo d la distancia entre rendijas consecutivas. Pero a 900 K, cada fullereno tiene una energía vibracional de unos 7 eV, almacenados es 174 modos vibracionales; cuatro de estos modos emiten radiación infrarroja de 7-19 μm, y durante los 3 ms de tránsito entre la red y la detección emiten de 2 a 3 de esos fotones infrarrojos. Mas su longitud de onda cumple $\lambda >> d$, y por tanto no permiten identificar la rendija atravesada. La figura 5 esquematiza lo dicho [12]. Otro tanto pasa con la radiación de cuer-

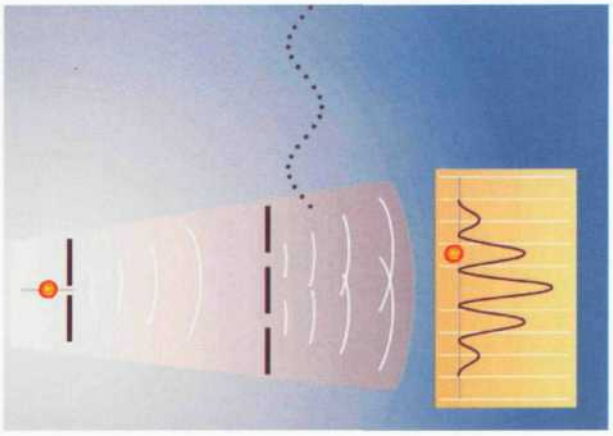

Fig. 5.– Esquema elemental del experimento de la doble rendija con fullerenos. La longitud de onda de la radiación emitida es grande en comparación con la separación entre rendijas adyacentes y no permite averiguar por qué rendija ha pasado la molécula.

[9] Echemos la cuenta. Para una bola de billar de masa m = 0,5 kg, por ejemplo, que se mueva sobre el tapete a 0,4 m/s, la longitud de onda λ de De Broglie vale $h/mv = 3 \times 10^{-33}$ m. No se conocen «orificios» ni «ranuras» de estas dimensiones para poder observar la difracción e interferencia de tales ondas. Incluso para cuerpos tan livianos como una mota de polvo (m ~ 1 μg), y velocidades tan pequeñas como las provocadas por agitación térmica debida al fondo cósmico de microondas (T ~ 3 K, v ~ 10^{-7} m/s), resulta λ ~ 10^{-18} m.

[10] Esta subsección, así como la dedicada al principio de indeterminación y a la discretización, son reflejo casi literal, con algunas aclaraciones, de otras contenidas en el capítulo sobre Física Cuántica del libro *Física 2*, de A. Galindo, A. Moreno, A. Benedí y P. Varela, McGraw-Hill, 1998.

[11] A. Zeilinger *et al. Nature*, octubre 14, 1999.

[12] Véase el artículo de A. I. M. Rae en *Nature*, octubre 14, 1999, para esta figura y comentarios.

po negro que cada fullereno caliente emite, y que es del orden de 0,1 eV durante su tiempo de vuelo por el trayecto, por lo que cada fotón asociado tiene como mínimo una longitud de onda de 10 μm >> d. La velocidad media de estos fullerenos del experimento fue de 220 m/s, y por tanto su longitud de onda de De Broglie era 2,5 pm, unas 400 veces menor que su diámetro de ~ 1 nm. Es posible que este tipo de experimentos pueda extenderse a sistemas más grandes, como macromoléculas e incluso virus [13].

El principio de indeterminación

En la física clásica, conociendo las posiciones y momentos iniciales de cada una de las partículas de un sistema, podíamos en principio predecir con exactitud cuáles iban a ser esas magnitudes un rato más tarde. Ya no; para empezar, un principio de indeterminación, debido a Heisenberg, impide que podamos medir con precisión arbitraria y a la vez una variable de posición y la correspondiente variable del momento. O una u otra; debemos conformarnos con conocer sólo una mitad de las variables que clásicamente estaban a nuestro alcance.

Un ciudadano normal alberga pocas dudas sobre la posibilidad de medir a la vez la posición de una moto y su velocidad; por eso encuentra natural que en la notificiación de una multa de tráfico por exceso de rapidez le señalen ambos datos. En un mundo hipotético en que la constante de Planck tuviese un valor parejo al de la acción de una avioneta en vuelo durante 1 s, por ejemplo, $h \sim 10^6$ J s,[14] el agente de policía tendría que renunciar o al lugar o a la celeridad, pues, como consecuencia del principio de indeterminación de Heisenberg que vamos a discutir, medir la velocidad de la moto con precisión de 10 km/hora exigiría desconocer su localización en aproximadamente 2 km. Y eso porque en tan extraño escenario la mera iluminación transversal del motorista con un solo fotón de ondas de radio de $\lambda \sim 1$ m para verle al pasar con precisión de 1 m podría transferirle momento más que suficiente para desviarle peligrosamente de su trayectoria.

Vivimos, sin embargo, en un Universo en el que el cuanto de acción es pequeño a escala ordinaria, y los efectos del principio de indeterminación se dejan notar sobre «motoristas» mucho más livianos: electrones, protones, núcleos atómicos, moléculas, etcétera.

Tras un cuidadoso análisis de los procedimientos de medida de magnitudes básicas como posición, momento y energía, Heisenberg enunciaba en 1927 su famoso principio de indeterminación. Este principio de incertidumbre limita las precisiones con que se pueden medir simultáneamente sobre una partícula pares (A,B) de magnitudes conjugadas tales como (x, p_x) : $\Delta A \Delta B \geq \frac{1}{2}\hbar$.

La razón de las relaciones de indeterminación reside en la dualidad onda-partícula. Por ejemplo, para ver dónde está una cosa con precisión Δx, lo normal es iluminarla con luz de longitud de onda $\lambda \leq \Delta x$, pero los fotones intercambian energía y momento con ella (efecto Compton), lo que conlleva una imprecisión $\Delta p_x \sim h/\lambda \geq h/\Delta x$.

Quizá la consecuencia más distinguida del principio de indeterminación sea la estabilidad de la materia: clásicamente los electrones atómicos son como pequeñas antenas radiantes que deberían caer sobre el núcleo en tiempos de unos pocos ps, haciendo inestables los átomos. El principio de indeterminación viene a su rescate, posibilitando de este modo la existencia de la tabla periódica y toda la riqueza estructural de la física atómica y molecular: al caer los electrones, se confinarían más; esto obligaría cuánticamente a aumentar su energía cinética, contrarrestando así la caída.

Discretización

Otro aspecto muy notable de la física cuántica es la discretización en los valores de ciertas magnitudes clásicamente continuas (energía, momento angular, ...). Sistemas simples como los átomos, moléculas y núcleos exhiben espectros de energías (colecciones de energías posibles) con partes discretas. Son como sus «notas» o «vibraciones» características, y se llaman niveles energéticos. La pequeñez del quantum de acción h de Planck relativa a los valores típicos de la acción clásica impide discernir la cuantización de la energía y de otras magnitudes en la vida ordinaria.

El enredo

El enredo o enmarañamiento es quizá la más sorprendente distinción de los quanta. Introducido el «enredo» por Schrödinger en 1935 para denotar superposición lineal de estados factorizables de varias partículas, se refería a él diciendo que «no era *un* sino *el* rasgo característico de la MQ». Einstein no soportaba sus consecuencias de aparente acción instantánea a distancia. De *spooky action at a distance* hablaba Einstein en una carta a Born. De «vudú» cuántico lo ha calificado Bennett.

El enredo consiste en tener un sistema bipartito 1+2 en un estado definido, sin que ninguna de las partes 1 y 2 lo tenga. Clásicamente el enredo no existe; pero en la MQ, en que los estados son una red de potencialidades como hemos dicho, es posible tener un estado en que eventualidades E_1, E_2 de las partes 1 y 2 estén individualmente indefinidas, pero correlacionadas entre sí, de modo que al actualizarse en sendas medidas, siempre sean las dos falsas, o las dos correctas.

Un estado enredado por antonomasia es el estado singlete de dos partículas de spin ½ : $2^{-1/2}(\uparrow\downarrow - \downarrow\uparrow)$. Las dos par-

[13] La difracción de helio por una red similar ha permitido medir recientemente *(Physical Review Letters,* septiembre 11, 2000) la longitud de enlace de las moléculas diatómicas más grandes y menos ligadas, a saber, moléculas $^4He_2$. Su energía de ligadura es de unos 10^{-7} eV, y la longitud de enlace de unos 50 Å.

[14] Esta acción macroscópica es también parecida a la desarrollada por un ciclista en una etapa contra-reloj a lo largo de un par de kilómetros.

tículas tienen sus polarizaciones correlacionadas: si el spin de una apunta en una dirección, el de la otra lo hace en la opuesta. Ninguna de ellas tiene un estado definido; la información del estado reside en correlaciones no locales esparcidas por todo, sin que ninguna medida local sobre una de las partes por sí sola pueda revelarla. Si la partícula 1 vuela hacia Zaragoza y la 2 hacia Sevilla, lugares en que nuestros colegas físicos miden sus estados de polarización, los resultados, aunque aleatorios para cada uno, están en perfecta correlación mutua $\uparrow \Leftrightarrow \downarrow$, $\downarrow \Leftrightarrow \uparrow$. Y esto se cumple, por muy separados que estén entre sí los físicos que comparten el par [15].

¿Transmisión superlumínica?

¿Cabe utilizar esto para enviar información de Zaragoza a Sevilla a velocidad superlumínica? Sí, si los físicos de Zaragoza supieran conseguir que los bits de polarización que obtienen codificasen un mensaje significativo. Pero no es así, pues las leyes cuánticas garantizan que cada muestra de bits obtenida en Zaragoza es absolutamente aleatoria. Si se selecciona un subconjunto de la misma para codificar información, por ejemplo una secuencia seguida de tres 1's si queremos transmitir el número primo 3, en Sevilla medirán en esos lugares tres 0's. Pero habrá que decirles (teléfono, correo electrónico, etc.) a qué lugares deben fijarse si queremos que identifiquen la información del 3. Y que sepamos, nadie sabe hacer superlumínico este último paso de la comunicación.

Si la clonación general de estados cuánticos fuera posible [16], el enredo podría ser usado para la transmisión superlumínica de información: pues en Zaragoza podrían medir la polarización de sus miembros de los sistemas enredados siguiendo un mensaje binario ($0 \leftrightarrow \pm_z$, $1 \leftrightarrow \pm_x$), lo que instantáneamente haría que los comiembros en Sevilla se polarizasen en las direcciones opuestas; su clonación haría posible a los colegas sevillanos determinar con fidelidad estas polarizaciones y, por tanto, leer el mensaje.

El enredo juega un papel central en las investigaciones actuales sobre información y computación cuánticas.

Consecuencias del enredo

El enmarañamiento es responsable de algunas de las predicciones más peregrinas de la MQ. El siguiente ejemplo (adaptado de uno similar de John Preskill [17]) ilustra lo extraño que es el mundo cuántico.

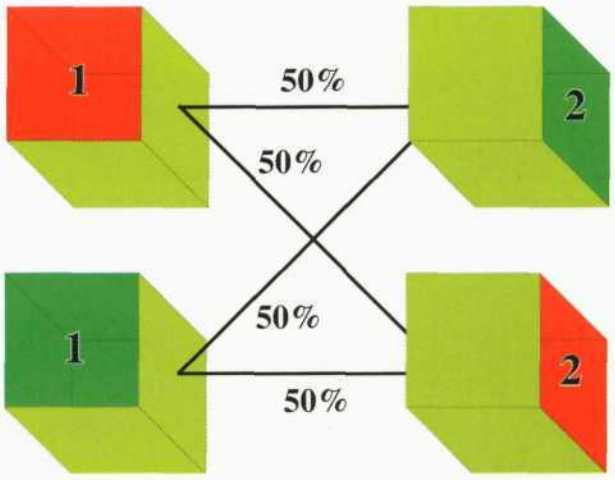

Fig. 6.– Representación de las cajas, con las puertas 1 y 2, y el reparto por igual en el color de fondo al cambiar de puerta.

Fig. 7.– Estado inicial de las cajas.

Supongamos tres cajas, una en Zaragoza, otra en Madrid, y otra en Sevilla. Cada caja tiene tres puertas, 1 (frontal), 2 (lateral) y 3 (superior), y su interior aparece de color rojo o verde al abrir cualquiera de ellas. Según qué puerta se abra, el color puede cambiar, de acuerdo con estas reglas: si vemos un interior rojo (verde) al abrir una de las puertas, al cerrarla y volverla a abrir de nuevo seguimos viendo el rojo (verde); pero si, tras conocer el color interior al abrir por una puerta, cerramos ésta y optamos seguidamente por destapar otra puerta distinta, un 50% de las veces vemos que el interior es rojo, y en el otro 50% restante, verde (figura 6).

Supongamos que se ha preparado el conjunto de interiores en estas «curiosas» cajas en un estado especial, en el que al abrir las tres por la puerta superior (puerta 3) aparecen sus interiores o todos rojos, o todos verdes, con igual amplitud de probabilidad (figura 7) [18].

Experimentalmente se comprueba sobre ese estado que si en una caja se abre la puerta 1 y en las otras dos cajas la

[15] Estas correlaciones máximas se han observado en pares enredados de fotones separados a distancias de 10,9 km (entre las localidades suizas de Bellevue y Bernex). Los fotones se produjeron en Ginebra y llegaron por fibra óptica de la Swiss Telecom a esos pueblos próximos a Ginebra (a 4,5 y a 7,3 km de Ginebra, respectivamente). Este experimento muestra que, con extremo cuidado en el manejo experimental, las correlaciones no disminuyen con la distancia.

[16] Como veremos luego, la linealidad/unitariedad de la MQ prohíbe la clonación cuántica: ¡no existen fotocopiadoras cuánticas!

[17] J. Preskill, conferencia titulada *Quantum Information and Quantum Computation*, 15 de enero de 1997, en http://www.theory.caltech.edu/people/preskill/index.html.

[18] El estado cuántico de partida es del tipo GHZ (por Greenberger, Horne y Zeilinger), y puede escribirse de varias formas equivalentes que respaldan lo dicho sobre los resultados de este experimento imaginado:

$$|\psi\rangle \propto |r_3 r_3 r_3\rangle + |v_3 v_3 v_3\rangle \propto$$
$$|r_2 r_2 v_1\rangle + |r_2 v_2 r_1\rangle + |v_2 r_2 r_1\rangle + |v_2 v_2 v_1\rangle \propto$$
$$|r_1 r_1 r_1\rangle + |r_1 v_1 v_1\rangle + |v_1 r_1 v_1\rangle + |v_1 v_1 r_1\rangle$$

puerta 2, siempre se ve un número par (0 o 2) de interiores rojos e impar (1 o 3) de verdes (figura 8).

Ahora nos entra la curiosidad de saber *a priori* qué veremos si abrimos las tres cajas por la puerta 1. Y vamos a razonar del modo siguiente. Al abrir dos de las cajas (digamos la 1 y la 2) por la puerta 1 pueden ocurrir tres casos: los interiores respectivos son ambos verdes, ambos rojos, o uno rojo y el otro verde. a) Supongamos que ambos son verdes. En virtud del hecho experimental antes citado, los interiores por la puerta 2 de las cajas 2 y 3 (1 y 3) deben ser ambos del mismo color, y por tanto también los de las cajas 1 y 2, lo que a su vez exige que el interior de la caja 3 por la puerta 1 sea verde. b) Si los interiores de las cajas 1 y 2 por la puerta 1 son rojos, los de las cajas 2 y 3 (1 y 3) por la puerta 2 deben ser de distinto color, y por tanto iguales los de las cajas 1 y 2, con lo que concluimos de nuevo que el interior de la caja 3 por la puerta 1 deber ser verde. c) Finalmente, si los interiores de las cajas 1 y 2 por la puerta 1 son distintos, digamos rojo en la 1 y verde en la 2, los de las cajas 2 y 3 (1 y 3) por la puerta 2 deben ser de distinto (igual) color, y por tanto distintos los de las cajas 1 y 2, de donde inferimos que el interior de la caja 3 por la puerta 1 deber ser rojo.

En cualquier caso, pues, podemos afirmar por nuestra argumentación teórica que al abrir las tres cajas por la puerta 1 veremos un número par de interiores rojos (figura 9).

Comprobémoslo ahora experimentalmente ...¡Vaya, pero si sale todo lo contrario! ¡Siempre se ve a través de las tres puertas 1 un número impar de interiores rojos! (figura 10).

¿Dónde falla el argumento? Sólo hay algo que hemos supuesto tácitamente: que la observación de los interiores de dos de las cajas no altera el interior de la otra [19]. Y para más respaldo interno a esta hipótesis, podemos pensar en llevar cada una de las tres cajas a una galaxia diferente (la 1 a Andrómeda, la 2 a la Gran Nube de Magallanes, y la 3 la dejamos en nuestra galaxia), y destapar las tres a la vez, de modo que no haya tiempo a que la información de lo visto en alguna de las cajas llegue a las otras. ¿Cómo va a «influir» el abrir la caja 2 en la Gran Nube de Magallanes sobre el color interior (por cualquiera de sus puertas) de las caja 1 en Andrómeda y 3 aquí? Es absurdo pensarlo, ¿no? Pues sí, será todo lo absurdo que nos parezca, pero de hecho esa «fantasmagórica acción a distancia», esa inesperada coordinación no local, forma parte de las leyes de la naturaleza, y se da en el extraño mundo de los quanta.

Este experimento, por sí solo, bastaría para mostrar que la MQ es incompatible con el realismo local. Queramos o no, la MQ es extraña y antiintuitiva. Decía Bohr: «Quien

Fig. 8.– Ilustración de la observación experimental de que al abrir dos puertas 2 y una 1, siempre se ve un número par de interiores rojos.

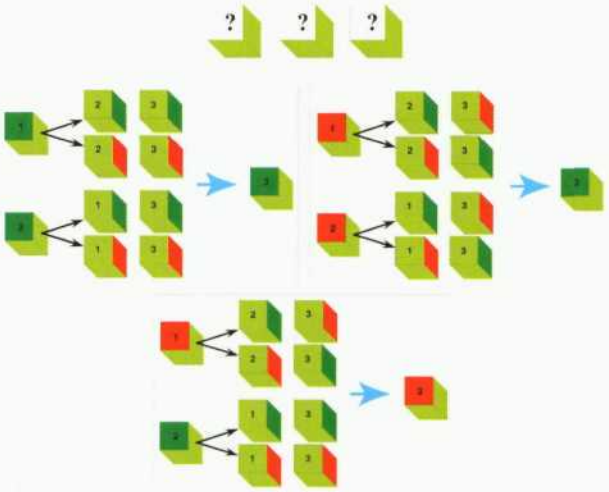

Fig. 9.– ¿Qué veremos al destapar las 3 cajas por la puerta 1? ¡Clásicamente, siempre un número par de fondos rojos!

Fig. 10.– ¡Cuánticamente, siempre un número impar de rojos!

no se sienta perplejo ante la MQ es que no la ha entendido bien».

¿Entender la MQ? Una cierta insatisfacción colectiva

Nadie presume de entender la MQ. Todo lo contrario. Los más grandes físicos de este siglo (Bohr y Einstein) y otros también preclaros (Bell, Feynman, Gell-Mann y Weinberg) se han mostrado perplejos y nerviosos ante las sutiles fintas dialécticas que propician los quanta [20]. Ninguno niega su enorme éxito para explicar cuantitativamente los fenómenos conocidos tanto en la física de lo pequeño como en la física de la materia condensada. Y la mayoría de los físicos saben cómo aplicarla correctamente en esas situaciones. Pero cuando se intenta describir el comportamiento de un quantum individual, la extrañeza y el desconcierto se nos apoderan [21].

Tres cuartos de siglo no han sido suficientes para disipar todos las dudas que plantean los principios cuánticos a gran número de profesionales. Destaca como particularmente acérrimo o rebelde el problema de la medición:

[19] El color de un interior al abrir una puerta sería, por tanto, un elemento de realidad según el criterio de Einstein, Podolsky y Rosen.

[20] Durante las jornadas *Cajal on consciousness* (Zaragoza, 29/11/99-01/12/99), me decía Gell-Mann que ya por fin comprendía la MQ. Ante mi insistencia, matizaría que la entendía «prácticamente» toda.

[21] Véase A. Galindo, *Cien años de quanta, loc. cit.*

mientras la evolución de un sistema cuántico cerrado es unitaria, y por ende lineal, reversible y determinista, al actualizar potencialidades, como en una medición sobre el sistema, el estado de éste sufre generalmente el infame «colapso», o «reducción» [22], no unitario, irreversible y probabilista. ¿Son reconciliables ambos tipos de cambio?

La linealidad de la evolución de un sistema en entornos no reactivos (esto es, insensibles a los cambios del sistema) traslada la indefinición objetiva de los sistemas cuánticos a los aparatos de medida, contra toda evidencia práctica. El gato de Schrödinger es la ilustración pintoresca de este conflicto [23]. Se han ofrecido muchas soluciones a este problema: desde considerar evoluciones no lineales, que se percibirían sólo en sistemas de muchos grados de libertad, con la virtud de llevar en tiempos muy cortos cualquier combinación lineal de estados base del aparato macroscópico de medida (los correspondientes a posiciones definidas de sus agujas) a uno de ellos, hasta reemplazar la ecuación de Schrödinger por otra estocástica, de origen tal vez en la propia estructura del espacio-tiempo que se supondría siempre bien definida (como ajena a las peculiaridades cuánticas). Ninguna de estas propuestas ha fructificado, y algunos experimentos han impuesto límites muy rigurosos a una posible no linealidad en la MQ.

Una alternativa radical es la «interpretación del estado relativo» de Everett (1957), o «interpretación de muchos mundos» (modernizada en el formalismo de historias consistentes). En ella el problema que nos preocupa desaparece como por encanto; niega simplemente que se actualicen potencialidades. Hay un sistema cerrado global, el Universo, con un estado que evoluciona lineal y unitariamente. Dado un subsistema 1, y el subsistema resto 2 (del que los observadores formamos parte), al medir en el 1 una magnitud A que puede tener distintos valores $\{a_1, a_2, ...\}$, el Universo (y con él nosotros) se bifurca en una coleccción de «ramas» o alternativas en las que todos los que allí estamos vemos que esa magnitud A tiene uno solo de esos valores, digamos a_k. No hace falta «reducir» el estado; nuestro estado relativo (neuronal o de consciencia) en esa rama está ya dispuesto a ver sólo ese valor a_k. Pero existen otros observables, para los que la ramificación será distinta y también real. En estas nuevas ramas, el valor de A no estará bien definido, y los observadores en esas ramas tendríamos la incómoda sensación de ver las agujas del aparato que mide A en posiciones indefinidas, en estados «grotescos» como los del gato ni vivo ni muerto. Volvemos, pues, a lo de siempre. No hemos resuelto nada; sí, nos hemos arropado con una miríada de mundos gratuitos (en violación grosera del principio de Occam) donde esconder el problema, pero éste, imperturbable, regresa siempre.

Siendo pragmático, se puede despachar el asunto [24] de esta guisa. El sistema cuántico interactúa con el aparato de medir, que a su vez lo hace con el ambiente. Los tres, sistema, aparato y entorno, están enredados. Como los grados de libertad de este último, es decir, su microestado, no se controlan ni observan por lo general, hay que promediar tomando trazas sobre ellos. En la práctica, el ambiente induce descoherencia entre los «estados de la aguja» del aparato de medida, esto hace perder irremediablemente sus fases relativas, y arrastra con ello al colapso. Sin embargo, sigue abierta la cuestión central de cómo se pasa del «y» al «o», es decir, por qué el resultado de cada acto de medición es uno y no varios. ¿Será tal vez ajena a la física?

LOS QUANTA EN LA INFORMACIÓN

La información tiene naturaleza física. Se imprime en soporte físico (ya sea la pared de la cueva de Altamira, ya sea un disco magneto-óptico), se articula en vibraciones sonoras, hertzianas, etc., no puede transmitirse a velocidad superior a la de la luz en vacío, y está sometida a las leyes naturales, en particular a las reglas cuánticas. Precisamente éstas, a través de su linealidad (con el paso del bit al qubit), enmarañamiento de estados (subsistemas cuya individualidad queda difuminada en el todo), no-localidad (naturaleza holística de los estados) y principio de indeterminación (existencia de magnitudes físicas incompatibles) hacen posibles nuevas y poderosas herramientas de transmisión y tratamiento de la información, así como una eficiencia de cálculo realmente prodigiosa [25].

El avance ha sido notable en el ámbito de la criptografía (el arte de esconder la información), donde ha proporcionado sistemas absolutamente seguros para la distribución cuántica de claves. La naturaleza misma sale garante de la inexpugnabilidad del secreto: a mayor aleatoriedad, mejor seguridad. No sólo hay un alto interés militar y estratégico en esto. Nuestra sociedad gira cada vez más en torno a la información digital; ingentes cantidades de dinero se mueven virtualmente en transacciones bancarias cuya seguridad se apoya en sistemas de encriptado sobre los que el asedio es constante, e informes confidenciales y números personales de tarjetas de compra

[22] La reducción matemática del estado aparece como un *modus ponens* intranscendente en la formulación de la MQ con historias. Pero la unicidad de la actualización es, evidentemente, otro cantar.

[23] *Mesogatos* o gatos mesocópicos de Schrödinger ya se han producido en laboratorio: estados atómicos superposición lineal de estados localizados y separados a distancias de 80 nm, muy superiores a sus tamaños individuales de unos 7 nm, y a las dimensiones atómicas del orden de 0,1 nm.

[24] *For all practical purposes* (FPAP), como decía Bell en uno de sus últimos trabajos, en el que proponía prohibir el uso del término «medición» en toda discusión seria sobre MQ, y reemplazarlo por el de «experimento».

[25] En esta parte y en la subsección sobre criptografía cuántica se usa bastante material de A. Galindo, «Quanta e Información», *Revista Española de Física*, 14 (número especial: *Cien años de quanta*), págs. 30-48, 2000.

viajan por la red expuestos a la piratería organizada, con el consiguiente riesgo de que nuestra intimidad sea violada y nuestra economía sangrada por manos ajenas. De ahí el interés en el desarrollo de un sistema absolutamente seguro de protección de datos.

Irónicamente, los quanta no sólo hacen posible esta protección total, sino que ponen de manifiesto la vulnerabilidad de los criptosistemas basados en la existencia de problemas computacionalmente duros para los ordenadores clásicos, pero que dejan de serlo para los ordenadores cuánticos. Éstos se caracterizan por funcionar de acuerdo a las reglas cuánticas y por un paralelismo masivo que permite en principio abordar cálculos que, aun no siendo teóricamente vedados para los ordenadores actuales, exigirían de éstos no sólo un tiempo medido en eones, sino también una memoria que sobrepasaría la capacidad de todo el Universo. El desarrollo de la computación cuántica constituye en este momento uno de los campos más activos y punteros de investigación. No son pocos los problemas técnicos a resolver, relacionados con la extraordinaria fragilidad de la coherencia de los estados cuánticos. Pero al igual que la sociedad usuaria de los mastodónticos ordenadores de finales de los cuarenta, con miles de tubos de vacío y decenas de toneladas de peso, no se imaginaba que medio siglo después cualquier colegial dispondría de máquinas de calcular mucho más ligeras y potentes, somos por naturaleza optimistas *(man muss Optimist sein,* decía Planck) y queremos pensar que el ingenio de los científicos logrará vencer finalmente las dificultades para construir ordenadores cuánticos de potencia adecuada. Con ellos el hombre habrá dado un paso de gigante en el entendimiento de la naturaleza. Si el siglo que acaba puede llamarse siglo de la información, al próximo probablemente se le conocerá como el siglo de la tecnología cuántica.

Bits *versus* qubits

Sabemos que el bit («binary digit») clásico, o cbit, es la unidad de información clásica, la información almacenable en un registro con dos estados (bit). Tiene sólo dos valores posibles, 0 y 1 (realizables como estados de un condensador descargado y cargado, respectivamente).

La unidad de información cuántica es el qubit (bit cuántico), la información almacenable en un sistema cuántico cuyo espacio de estados es 2-dimensional (qubit). Por ejemplo, un spin 1/2, la polarización de un fotón, átomos con 2 estados relevantes, etc., son qubits.

Toda información clásica es codificable en binario. Por ejemplo, con 8 bits ($2^8 = 256$ posibilidades) tenemos de sobra para asignar un número en binario a cada signo del teclado y así digitalizar cualquier texto, por ejemplo, el Quijote, representándolo por una cadena de bits o por una cadena de condensadores cargados/descargados. Midiendo la carga de éstos podemos reconstruir la obra de Cervantes.

Con qubits haríamos lo mismo, pero con un cuidado extremo a la hora de leer. Porque si, por ejemplo, los estados base $|0\rangle$, $|1\rangle$ de los qubits con que salvamos el Quijote son $|+\rangle_z$ y $|-\rangle_z$, pero luego a la hora de leer nos equivocamos y medimos polarizaciones $|+\rangle_x$ y $|-\rangle_x$, los resultados obtenidos serán aleatorios, el Quijote será irreconocible, y lo que es peor, no habrá manera de deshacer el entuerto, siendo preciso codificar de nuevo la genial novela. Por tanto, los bits son robustos, y los qubits muy frágiles. La obtención de información sobre un sistema cuántico generalmente lo perturba.

Otra distinción importante entre los elementos de información clásicos y cuánticos está en el proceso de copiado. Cualquier estado clásico de un sistema es copiable; estamos hartos de verlo (copias de un modelo prototipo, de una efigie, de una fotografía, de un escrito, de un fichero digital, etc.). Supongamos, sin embargo, que queremos copiar un estado cuántico. Puede ocurrir que conozcamos dicho estado (por ejemplo, que es un electrón moviéndose con tal momento y polarizado en tal dirección) y entonces esta información basta para preparar otro sistema en ese mismo estado. Si por contra desconocemos el estado a copiar, estamos perdidos, pues con el único ejemplar que nos dan ningún conjunto de medidas compatibles (salvo las que dejaran el estado incólume, y que evidentemente ignoramos cuáles son) puede revelarnos toda la información necesaria para determinar el estado y así poderlo reproducir. En el caso clásico, al contrario, podemos medir sobre el sistema cuanto necesitemos para su copia macroscópica, sin deterioro apreciable del estado a reproducir.

La imposibilidad de clonación cuántica, que demostraremos a continuación, tiene virtudes esenciales para proteger la información (criptografía), o para evitar la falsificación de moneda (billetes cuánticos).

Hay otras diferencias más profundas y con mayor impacto potencial tecnológico. El número de estados codificables con N bits es 2^N, y cada uno queda fijado a través de sólo un número binario. Pero el número de estados codificables con N qubits es infinito, a saber, cualquier combinación lineal de los 2^N estados base, y por tanto, su especificación requiere conocer 2^N amplitudes. Para $N = 300$, este número es del orden del número de grados de libertad del Universo visible. Luego es de esperar que un ordenador que opere sobre qubits podrá en principio realizar hazañas impensables para un ordenador clásico.

Finalmente, la sutileza del enredo, de la posibilidad de esconder la información difuminándola de modo que ninguna medición local pueda revelarla, ofrece también posibilidades nuevas a la información. Por ejemplo, en el enredo se fundamentan algunos protocolos cuánticos, unos de aplicación en criptografía y corrección de errores para la computación cuántica, y otros sin análogo clásico, como la codificación cuántica densa, y la teleportación cuántica (que no tenemos tiempo de discutir aquí).

Clonación cuántica

No es posible clonar de forma exacta estados cuánticos no ortogonales. Seré más preciso:

1. La linealidad de la MQ exige que no existan dispositivos que puedan clonar estados cuánticos desconocidos y arbitrarios.
2. La unitariedad de la evolución en MQ implica que no es posible clonar estados cuánticos distintos y no ortogonales.

En efecto (figura 11):

1. Si existiera una máquina lineal Φ tal que $\Phi : \psi_0\alpha \rightarrow \psi_\alpha\alpha\alpha$, para todo estado α, tendríamos que, por un lado, $\Phi : \psi_0(\alpha+\beta) \rightarrow \psi_{\alpha+\beta}(\alpha+\beta)(\alpha+\beta)$, mientras que por otro $\Phi : \psi_0(\alpha+\beta)=\psi_0\alpha+\psi_0\beta \rightarrow \psi_\alpha\alpha\alpha + \psi_\beta\beta\beta$. Contradicción.
2. Si existiera una máquina unitaria Φ tal que $\Phi : \psi_0\alpha \rightarrow \psi_\alpha\alpha\alpha$, $\psi_0\beta \rightarrow \psi_\beta\beta\beta$, para todo par de estados α, β, tendríamos que $|(\beta, \alpha)| = |(\psi_0\beta, \psi_0\alpha)| = |(\Phi(\psi_0\beta), \Phi(\psi_0\alpha))| = |(\psi_\beta\beta\beta, \psi_\alpha\alpha\alpha)| = |(\psi_\beta, \psi_\alpha)||(\beta\beta, \alpha\alpha)| \leq |(\beta\beta, \alpha\alpha)| = |(\beta, \alpha)|^2$, y como $|(\beta, \alpha)| \leq 1$, forzosamente $|(\beta, \alpha)| = 0,1$.

Aunque no sabemos cómo clonar un estado desconocido $a|0\rangle + b|1\rangle$, sí es posible conseguir estados de la forma $a|00...0\rangle + b|11...1\rangle$. Si Φ es una máquina lineal capaz de clonar estados $|0\rangle$, y $|1\rangle$, (fácil, pues de estos estados conocemos su preparación), basta aplicar dicha Φ al estado $a|0\rangle + b|1\rangle$.

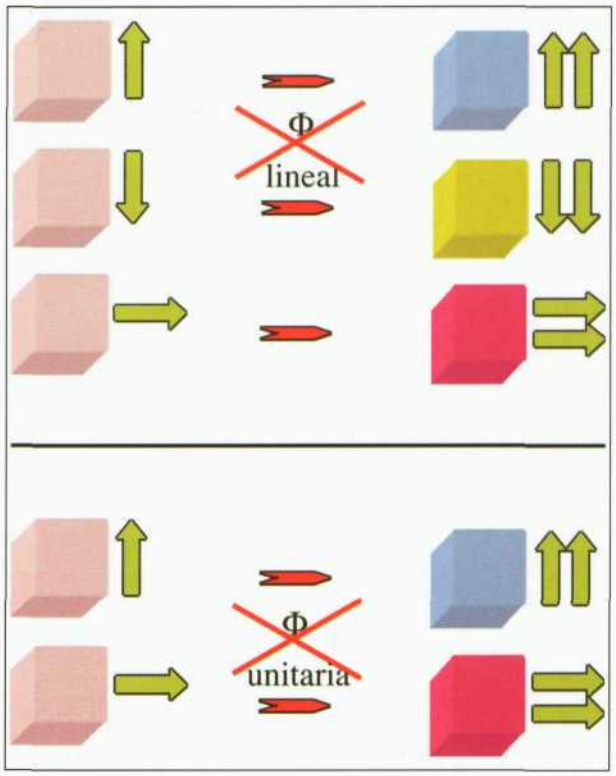

Fig. 11.– Ilustración de la imposibilidad de clonar estados cuánticos, tanto por la linealidad, como por la unitariedad. La caja denota la presunta fotoQopiadora, y su color indica el estado en que se encuentra.

QRIPTOGRAFÍA

La criptología hunde sus raíces en el pasado. Ya en el siglo V a. C. los militares de Esparta transmitían y descifraban mensajes secretos; precisamente uno de éstos, roto por Gorgo, esposa de Leónidas, llevaría a éste al paso de las Termópilas para detener, al frente de los espartanos, y con el sacrificio de su vida, el cruce de las tropas persas.

María Estuardo, reina de Escocia, perdió su cabeza porque Sir Francis Walsingham (fundador del Servicio Secreto británico) descifró un mensaje en clave donde se hablaba de planear la muerte de Isabel de Inglaterra, y Estados Unidos entró en la Primera Guerra Mundial porque los servicios de inteligencia ingleses descifraron un telegrama de Zimmermann en que ofrecía ventajas territoriales a México si se aliaba con Alemania.

Pero es a mediados de este siglo, en la década de los cuarenta, cuando se convierte la criptografía en parte de la teoría de la información a través de los trabajos seminales de Shannon.

La criptografía trata de transformar información haciéndola ininteligible para quienes no estén autorizados para lo contrario. Las estrategias desarrolladas por estos últimos para desvelar la información oculta constituyen el criptanálisis, y el conjunto de actividades de ambos mundos opuestos y en continua pugna forma la criptología.

Criptología elemental

El cifrado cesáreo (atribuido a Julio César) es un *cifrado de transposición:* cada signo se desplaza una misma cantidad a lo largo del alfabeto (módulo la longitud de éste). Así

QR NRLNRB YORQRP

no es más que

TU QUOQUE BRUTUS

con una transposición de –3 aplicada a éste.

El criptosistema CÉSAR es sumamente vulnerable por cualquier aficionado, pues basta aplicar todas las transposiciones posibles hasta conseguir algo que tenga sentido [26].

Los aficionados a las novelas policíacas recuerdan seguramente cómo Sherlock Holmes, en el relato *The Adven-*

[26] Sin embargo, a César pudo servirle para comunicarse con su amigo Cicerón y otros.

ture of the Dancing Men, descifra cinco mensajes (figura 12) a partir de las 62 figuras que los integran (estudiando su frecuencia, pues se sabe, por ejemplo, que en inglés la E es la letra más frecuente, incluso en textos cortos) y con ello cifra otro (COME HERE AT ONCE) mediante el cual atrae a un peligroso gángster de Chicago a donde le espera la policía.

Este procedimiento se conoce como *cifrado con sustitución monoalfabética*. No es tampoco nada seguro, a pesar de que el número de ensayos ciegos es mucho mayor que para el cifrado de transposición. Se le ataca de modo algo más sutil, estudiando, como en el caso anterior, las frecuencias de los distintos símbolos. En inglés, del análisis de unas 100.000 letras de texto de diversas fuentes, se ha visto que las frecuencias (en %) de las distintas letras del alfabeto son las representadas en la figura 13.

Los criptanalistas profesionales se apoyan también en la distribución frecuencial de poligramas (conjuntos de varias letras contiguas en el texto), generalmente digramas y trigramas, para destripar la clave de sustitución. Se sabe, por ejemplo, que en inglés los digramas más frecuentes son, de más a menos, TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ..., y en cuanto a los trigramas, THE, ING, AND, HER, ERE, ENT, THA, NTH, ...

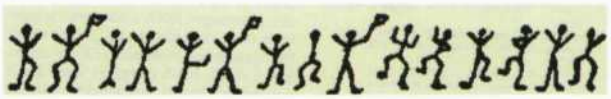

Fig. 12.– Primero de los criptogramas analizados por Sherlock Holmes. Las banderas en algunas figuras indican sólo separación de palabras. Dice: AM HERE ABE SLANEY.

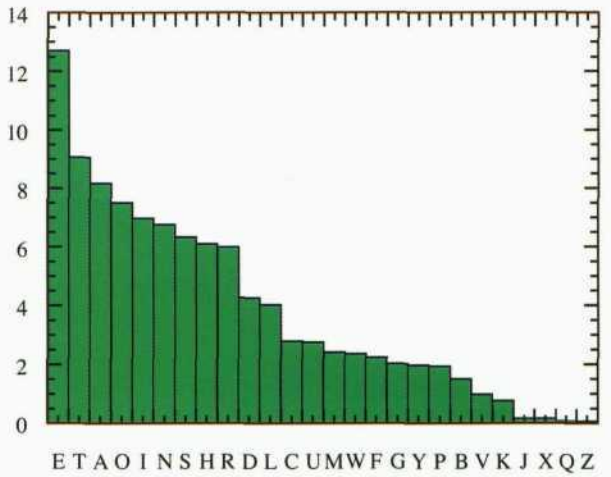

Fig. 13.– Frecuencias (en %) de las letras en inglés, ordenadas de mayor a menor.

Criptografía clásica

Como dijimos antes, la criptografía forma parte importante de la teoría de la información desde 1949, a partir de los trabajos pioneros de Shannon en los Bell Labs. Probó éste que existen cifrados inexpugnables, o sistemas de secreto perfecto. De hecho, alguno de éstos se conocía desde 1918 (mas no que fuera inquebrantable): el sistema *one-time pad* (ONETIMEPAD), o de cuaderno de un solo uso. Se conoce también como cifrado VERNAM, pues fue ideado por el joven ingeniero Vernam (de la ATT) en diciembre de 1917 y propuesto a la compañía en 1918; con el sistema de Vernam se automatizaba por vez primera tanto el cifrado como el descifrado de los mensajes.

Cuaderno de «usar y tirar»

El cifrado basado en un cuaderno con hojas de un solo uso consiste en que el texto *ordinario* a cifrar se convierte en una sucesión de números $p_1, p_2, ..., p_N$, y luego se usa una *clave* $k_1, k_2, ..., k_M$, $M \geq N$, de números aleatorios con los que se combinan aquéllos en aritmética modular $p_j + k_j = c_j \bmod B$, donde B es el número máximo de símbolos distintos (2 en binario, 10 para dígitos, 28 para letras, etc.), para producir un texto *cifrado* o *criptograma* $c_1, c_2, ..., c_N$. Tanto el que escribe (Alice) como el destinatario (Bob) tienen que tener la misma clave de números aleatorios, de modo que al recibir Bob el criptograma, deshace el algoritmo con esa clave y así recupera el texto original.

Posibles frecuencias en el texto fuente (en las que se apoyan los quebrantacódigos para descifrar) quedan borradas por la clave aleatoria.

La longitud de la secuencia de aleatorios debe ser mayor o igual que la del texto fuente, y no debe usarse más de una vez [27]. Shannon demostró que si la clave es de menor longitud que el texto es posible extraer información del mensaje cifrado. Estos requerimientos hacen muy gravoso el procedimiento cuando es mucha la información a encriptar. Además no es fácil disponer de secuencias de números verdaderamente aleatorios.

Este sistema de cifrado fue usado por diplomáticos alemanes y rusos en la Segunda Guerra Mundial, y por el espionaje soviético durante la guerra fría. Su nombre popular de «one-time pad» se debe a que las claves estaban escritas en un cuaderno o bloc, y cada vez que se utilizaba una, se arrancaba la correspondiente hoja del cuadernillo donde figuraba y se destruía. Se cuenta que el uso continuado de la misma clave permitió desenmascarar la red de espionaje de los Rosenberg y al espía atómico Fuchs. También lo usó el «Che» Guevara para comunicarse en clave desde Bolivia con Fidel Castro. Y es rutina para las comunicaciones a través del «teléfono rojo» entre la Casa Blanca y el Kremlin.

[27] Interceptados dos mensajes cifrados con la misma clave, su suma módulo 2 elimina ésta y hace posible desencriptar con cierta facilidad los mensajes.

Aunque invulnerable, el criptosistema VERNAM tiene el inconveniente de exigir claves tan largas al menos como el texto a cifrar. Por eso se usó únicamente para cifrar información sumamente valiosa, reemplazándose para menesteres menos delicados por encriptación con claves más cortas aunque quebrantables. Precisamente el acicate por romper mensajes secretos propiciaría el desarrollo de los ordenadores.

Sistema PKC

De aquí el interés del PKCS *(Public Key Cryptographic System),* ideado a mediados de la década de los setenta por Diffie y Hellman en Stanford, implementado en el MIT por Rivest, Shamir y Adleman [28], y de uso muy frecuente, por ejemplo en Internet.

Se basa en el uso de dos claves: la persona X da una clave pública, a disposición de cualquiera, y otra privada que no da a conocer, y que es la inversa de la anterior. La primera la utiliza cualquier persona R para mandarle a X mensajes cifrados; cuando X los recibe, los descifra con su clave privada. Es claro que esto sólo tiene interés si exclusivamente X sabe deshacer el cifrado.

¿Cómo se consigue esto? De una forma sutil e inteligente: el sistema PKC utiliza, para encriptar mensajes, funciones de dirección única (o unidireccionales) con «trampilla», es decir, funciones inyectivas de complejidad P, es decir, *tratables* (computacionalmente), cuyas inversas son prácticamente *intratables* [29], esto es, muy costosas de evaluar salvo si se dispone de información adicional como algún certificado sucinto (problema NP) [30]. Entre estas funciones inversas destacan la factorización de enteros, y el cálculo de logaritmos discretos en cuerpos finitos y sobre curvas elípticas. El sistema PKC se permite el lujo de dejar a la vista pública tanto el algoritmo de encriptación como media clave sin que se resienta en la práctica su seguridad; contrasta ostensiblemente con el sistema DES, donde a pesar de hacerse público sólo el algoritmo, su vulnerabilidad ha quedado demostrada.

Sistema RSA

Uno de los modos más interesantes de implementación del PKCS es el método RSA (Rivest, Shamir, Adleman), basado en la dificultad de factorizar números grandes. Se usa, en particular, para proteger las cuentas electrónicas bancarias (por ejemplo, frente a transferencias bancarias ordenadas por vía electrónica).

La clave pública de X consiste en un par de números enteros $(N(X), c(X))$, el primero muy grande, digamos de 200-300 dígitos, y el otro en el intervalo $(1, \phi(N(X)))$ y coprimo con $\phi(N(X))$, siendo ϕ el indicador o función indicatriz de Euler ($\phi(n)$ es el número de coprimos con n en el intervalo $[1,n]$).

Tras transformar el remitente R su mensaje M en secuencia de números (binarios, decimales, o en la base que se convenga), lo rompe en bloques $B<N(X)$ de la mayor longitud posible, cifra cada bloque B según

$$B \rightarrow C := B^{c(X)} \bmod N(X)$$

y manda la secuencia de criptogramas $C(B)$ a X. Denotemos esta operación de cifrado como $M \rightarrow P_X(M)$, indicando por el símbolo P_X que se ha hecho con la clave pública de X.

El destinatario X descifra cada $C(B)$ como

$$C(B) \rightarrow B := C(B)^{d(X)} \bmod N(X)$$

donde el exponente $d(X)$ para el descifrado es la clave privada, y que no es otro que la solución a

$$c(X)d(X) = 1 \bmod \phi(N(X))$$

Esa solución es

$$d(X) = c(X)^{\phi(\phi(N(X)))-1} \quad \bmod \phi(N(X)).$$

El descifrado lo indicaremos por $P_X(M) \rightarrow S_X(P_X(M)) = M$, donde el símbolo S_X alude a la clave privada o secreta de X.

En principio, cualquiera puede calcular $d(X)$, pues se conocen $c(X)$ y $N(X)$, y así romper el secreto. Y aquí es donde entra ahora la astucia de X. Para ponérselo pero que muy difícil a Eve (nombre convencional del personaje que efectúa la escucha no autorizada) mejor es que se atenga a ciertas normas, entre las que destacan las siguientes:

- Debe X escoger el módulo $N(X)$ como producto de dos primos enormes y aleatorios (de al menos un centenar de dígitos cada uno) p_1, p_2, y no muy próximos entre sí (basta que las longitudes de sus expresiones difieran en unos pocos bits), pues de lo contrario a Eve, que conoce $N(X)$, no le costaría mucho encontrar dichos factores. Hay que evitar tomar primos que estén en tablas o sean de formas muy especiales.

[28] Parece ser que algunos años antes que Diffie y Hellman el Servicio Secreto Británico conocía este sistema, pero como material clasificado (secreto militar).

[29] No se conocen funciones verdaderamente unidireccionales; las hay, sin embargo, que probablemente lo sean, y que lo son en la práctica con los algoritmos conocidos hasta el momento.

[30] Problemas de clase P son, por ejemplo, la multiplicación de enteros, la ordenación, el cálculo del determinante de una matriz, y la exponenciación en aritmética modular. Quizá también lo sea la prueba de primalidad.

- Como X conoce p_1, p_2, sabe ya calcular $\phi(N(X))$ como $(p_1 - 1)(p_2 - 1)$. Ahora tiene que escoger X un entero $d(X)$ (su clave privada) al azar en el intervalo $(1, \phi(N(X)))$, coprimo con $\phi(N(X))$, y calcular la clave pública $c(X)$ mediante $c(X) = d(X)^{\phi(\phi(N(X)))-1} \bmod \phi(N(X))$, o mejor aún, usando el clásico algoritmo de Euclides.
- El número $d(X)$ no debe ser pequeño, para evitar que se pueda encontrar por prueba y error. Por eso conviene comenzar fijando la clave privada. Pero también hay que procurar que $c(X)$ no resulte demasiado pequeño, pues de lo contrario la interceptación de un mismo mensaje enviado a varios destinatarios con la misma clave pública aunque distintos módulos podría conducir sin mucho esfuerzo a su descifrado.

Cualquier persona que sólo conozca $N(X)$ pero no sus factores, aparentemente[31] tendrá primero que factorizar $N(X)$ para calcular $\phi(N(X))$, y con ello poder hallar el exponente para descifrar; pero factorizar un número de 250 dígitos le llevaría a una estación de trabajo de 200 MIPS unos 10 millones de años con el mejor algoritmo hoy conocido.

El sistema PKC permite también «autentificar» digitalmente los mensajes, y añadirles una «firma electrónica» o «digital».

Los números RSA

En 1977 Martin Gardner publicó un mensaje cifrado en sus *Mathematical Games* de *Scientific American* usando el método RSA, con la promesa de recompensar con 100$ (pagaderos por el grupo de Rivest et al. en MIT) a quien lo descifrara:

96869613754622061477140922254355882905759991124574319874695120930816298225145708356931476622883989628013391990551829945157815154

Este criptomensaje había sido obtenido a partir de una frase en inglés y el diccionario

$$\text{Espacio} \to 00,\ a \to 01,\ \ldots,\ z \to 26,$$

por el método RSA, y clave pública (RSA-129, 9007), donde RSA-129 era el siguiente número de 129 dígitos

RSA-129 =
114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541

El descifrado requería factorizar RSA-129 en sus dos factores primos de 64 y 65 dígitos cada uno. Se estimaba entonces que el tiempo para conseguirlo sería al menos de unos 4×10^{16} años. En 1994 nuevos algoritmos de factorización y el trabajo en red de un millar de estaciones de trabajo permitió lograrlo en unos 8 meses, tras un tiempo de cálculo de 5000 MIPS-años, mediante el algoritmo de la criba cuadrática (QS). Esos factores son

3490529510847650949147849619903898133417764638493387843990820577

×

3276913299326670954996198819083446141317764296799294253979828853 3

conociendo los cuales es inmediato hallar el mensajo original:

THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE

Dos años después se rompió el RSA-130 mediante el algoritmo de factorización más potente hasta la fecha: la criba general de cuerpos de números (GNFS), y en un tiempo de computación casi un orden de magnitud menor que el empleado para el RSA-129. Finalmente, en agosto de 1999 se ha ultimado la factorización del RSA-155, también mediante GNFS y tras unos 8000 MIPS-años. Tiene 512 bits y es producto de dos primos de 78 dígitos. Para darnos una idea de la magnitud de este problema, en su solución se han empleado 35,7 años de CPU para hacer la criba, repartidos entre unas trescientas estaciones de trabajo y PCs, y 224 horas de CPU de un CRAY C916 y 2 Gbytes de memoria central para hallar las relaciones entre las filas de una monstruosa matriz de 6,7 millones de filas y otros tantos de columnas, y una media de 62,27 elementos no nulos por fila.

Hace unos pocos años se daba como muy seguro el uso de módulos de 512 bits. Hoy, tras el desarrollo del algoritmo GNFS de factorización, se recomienda usar módulos de (768, 1024, 2048) bits para uso (personal, corporativo, y de extrema seguridad).

Si bien el problema de factorización sigue siendo en la actualidad un problema computacionalmente duro, nadie está seguro de que no pueda surgir el día de mañana algún matemático con un algoritmo radicalmente más rápido con el que los computadores clásicos existentes puedan factorizar en tiempo polinómico. De hecho, la computación cuántica ha despertado enormes expectativas en este sentido, con el algoritmo de Shor que luego comentaremos. ¡Por eso la CIA sigue de cerca los avances en teoría de los números y de la computación!

Criptografía cuántica

La física cuántica ofrece un método seguro para cifrar, garantizado por las propias leyes físicas. Ha nacido con

[31] «Aparentemente», porque se ignora si existen o no procedimientos alternativos para descifrar $C(B)$ que no pasen por la obtención del exponente inverso, o si el cálculo de éste exige forzosamente conocer los factores primos de N.

ello la *Qriptografía*. Se basa en los principios de complementariedad e incertidumbre, y en la indivisibilidad de los quanta. El pionero ha sido Stephen Wiesner, quien ya en 1969 sugirió, entre otras cosas, cómo fabricar billetes de banco infalsificables, billetes de banco cuánticos. A mediados de los ochenta Bennett y Brassard idearon un criptosistema cuántico basado en el principio de Heisenberg, que pronto se implementaría experimentalmente mandando con fotones polarizados información secreta a 30 cm de distancia. Este sistema (conocido como protocolo BB84) usa estados cuánticos no ortogonales para evitar su clonación por un posible escucha; por emplear 4 estados distintos, se llama también *esquema de cuatro estados*. El empleo de correlaciones cuánticas no locales con pares de fotones enredados por conversión paramétrica a la baja fue propuesto luego por Ekert; en este sistema serían las desigualdades de Bell las encargadas de proteger la seguridad. De ahí el calificativo de *esquema EPR*. Aquí nos limitaremos a comentar un protocolo de dos estados llamado B92 (Bennett 1992) y a mencionar brevemente las realizaciones experimentales de estas ideas.

Billetes con seguro cuántico

Un billete de banco a prueba de falsificadores podría ser un billete con un número, y una pequeña colección (digamos veinte) de fotones, aprisionados indefinidamente en celdas individuales de paredes perfectamente reflectoras, y con polarizaciones lineales secretas e individualmente aleatorias a 0°, 45°, 90° y 135° que el banco emisor guardaría en secreta correspondencia con el número de identificación (figura 14).

El banco, por tanto, podría en cualquier momento comprobar la legitimidad del billete, sin estropearlo, pues sabría cómo colocar los polarizadores para ver la polarización de cada fotón sin destruirla. Cualquier falsificador que intentase copiar un billete, sin embargo, desconocedor de en qué direcciones se polarizaron los fotones, rompería la polarización inicial proyectándola en alguna de las dos correspondientes al polarizador que eligiera para medir.

QKD: distribución cuántica de claves

Si bien lo de los billetes cuánticos puede parecer una fantasía, no lo son los sistemas de distribución cuántica de claves de alguno de los tipos existentes, como los citados protocolos BB84 y B92. Proporcionan una forma de compartir dos personas claves absolutamente secretas, y por tanto es el complemento ideal al cifrado Vernam.

Fig. 14.– Billetes con seguro cuántico.

Alice y Bob quieren intercambiar información secreta, sin necesidad de intermediarios para llevar cuadernillos de claves de uno al otro, y sin temor a que rompan su código. Para ello deben compartir una clave, sólo conocida por los dos. Proceden según un protocolo de comunicaciones, o conjunto de pasos a seguir para o bien detectar cualquier escucha no autorizada, o en caso contrario para establecer la clave secreta que sólo ellos compartirán para cifrar y descifrar.

Protocolo B92, o esquema de dos estados

Este protocolo usa sistemas en dos estados no ortogonales. Consta de cuatro pasos.

- Paso 1: Alice y Bob generan sendas secuencias aleatorias de bits 0, 1. Por ejemplo:

```
Alice 1011111000111101011001010011101110010101l0...
Bob   0001010001110000101100111111010010010100000...
```

- Paso 2: Alice prepara estados de spin ½ asociados a cada uno de sus bits, de acuerdo con esta tabla:

$$0 \rightarrow A := |\uparrow\rangle \text{ (spin hacia arriba)}$$
$$1 \rightarrow D := |\rightarrow\rangle \text{ (spin hacia la derecha)}$$

Por ejemplo:

```
Alice 1011111000111101011001010011101110010101l0...
      DADDDDDAAADDDDADADDAADADAADDDADDDAADADADDA...
```

- Paso 3: Alice manda a Bob cada estado de spin que ha preparado por un canal cuántico (canal sin influencia del medio sobre los estados cuánticos), y Bob mide sobre ellos ya el proyector $P_{\text{Izquierda}}$, ya P_{aBajo}, según su propia secuencia de bits:

$$0 \rightarrow P_{\text{I}}$$
$$1 \rightarrow P_{\text{B}}$$

Por ejemplo:

```
Bob 0001010001110000101100111111010010010100000...
    IIIBIBIIIBBBIIIIBIBBIIBBBBBIBIIBIIBIBIIIII...
    NSNSNNNSSNSSNNSNNNNNSNNNNNSNSNNSNSNNNNSNNN...
```

y se apunta los resultados (S si el estado de spin «pasa la cuestión», N si el estado falla, es decir, no pasa la pregunta). Cuando el bit de Bob es distinto del de Alice, el resultado es siempre N. En los demás casos, un 50 % es S y el otro 50 % es N.

```
Alice 1011111000111101011001010011101110010101l0...
Bob   0001010001110000101100111111010010010100000...
      NSNSNNNSSNSSNNSNNNNNSNNNNNSNSNNSNSNNNNSNNN...
      -0-1---00-11--0-----0-----1-1--1-0----0---...
```

• Paso 4: Bob manda una copia pública de la secuencia de sus resultados (S, N) a Alice, pero no de los proyectores que ha medido. Cualquiera puede tener acceso a esta secuencia de resultados. Y tanto Alice como Bob mantienen sólo aquellos bits de sus secuencias para los que el resultado de Bob ha sido S:

```
Alice 10111110001111010110010100111011100101010110...
Bob   00010100011100001011001111101001001010000...
      -S-S---SS-SS--S-----S-----S-S--S-S----S---...
      -0-1---00-11--0-----0-----1-1--1-0----0---...
```

Luego la clave destilada es

```
0100110011100...
```

Estos bits mantenidos constituyen la clave binaria a compartir para cifrar (Alice) y descifrar (Bob) como tablilla de un solo uso. En media, la longitud de esta clave es la cuarta parte de cada secuencia inicial.

Efectos de una escucha

¿Qué ocurre si hay una escucha no autorizada por parte de Eve? Supongamos que Eve conoce los tipos de preparaciones y medidas que Alice y Bob van a hacer, pero no sus secuencias aleatorias iniciales. Supongamos asimismo que Eve puede entrar en el canal cuántico, y medir y/o modificar los estados que quiera de los que por allí pasan. Del canal público admitiremos que puede escuchar, pero no interferir (de lo contrario, podríamos echar mano de un protocolo de autentificación que permitiera a Alice saber que nadie ha cambiado la clave que le manda Bob, por ejemplo utilizando un trozo remanente de clave secreta no empleada con anterioridad).

En primer lugar, no cabe pensar en «pinchar»; si Eve pudiera clonar estados, le bastaría con hacerse copias de lo que pasa por el canal cuántico, sin alterar el original, para conocer los estados preparados por Alice y de ahí, tras escuchar el envío final de Bob, reconstruir la clave secreta. Pero la linealidad de la mecánica cuántica prohíbe la clonación de estados no ortogonales como los usados por Alice.

El análisis completo de los efectos de la escucha es largo y complejo. En el caso elemental de que Eve sea poco sofisticada y se limite a interceptar cada estado, actuar sobre él para intentar extraer información del mismo, y luego reemitir otro en su lugar, la escucha se manifiesta en la variación que produce en el ritmo de generación de la clave, y en la tasa de errores y proporción de 0 vs 1 en una porción de las S.

Supongamos, por ejemplo, que Eve decide medir P_A en cada uno de los estados que «escucha» de Alice, reenviando a Bob el estado resultante. Todos los estados A de Alice pasarán como A, pero también lo harán un 50% de los D de Alice (mientras el otro 50% pasarán como B). Luego Eve sólo es capaz de identificar con total certeza aquellos estados de Alice que pasan la medida de Eve como B (y por tanto son estados D de Alice), es decir, el 25% de todos los estados de Alice. Pero esto a costa de dañar el material clave de Alice y Bob: por ejemplo, Bob hallará una descompensación entre S y N; mientras en ausencia de escucha la proporción S:N = 1:3, con la escucha que hemos supuesto por parte de Eve la proporción pasa a ser S:N = 3:5.

Realización práctica de QKD

El protocolo BB84 se ha implementado por vez primera en Los Álamos (1989-1992) con fotones polarizados guiados por un tubo con aire de 32 cm.

En 1995 se realizó experimentalmente el protocolo B92, también con fotones polarizados, transmitidos esta vez a lo largo de una fibra óptica de 23 km uniendo bajo las aguas del lago Lemán las ciudades de Ginebra y Nyon. El uso de estados de polarización de fotones para largas distancias tiene un inconveniente, y es su pérdida en la transmisión por la fibra debido a que la birrefingencia en las partes no rectas de la fibra transforma los estados de polarización lineal en estados de polarización elíptica, y además produce dispersión de modos de polarización ortogonales. De ahí el interés en otros modos de codificar los estados, como por ejemplo mediante fases en lugar de polarizaciones. Un grupo de la British Telecom en el Reino Unido lo ha conseguido (1994) con fibra óptica a lo largo de 30 km, usando interferometría con fotones de fase determinada. No hay dificultades mayores en llegar hasta unos 50 km. Por eso puede ser usado para conectar con seguridad diversas agencias del Gobierno en Washington. Cubrir distancias superiores a 100 km requerirá el uso de repetidores seguros en los que se pueda generar material clave para la retransmisión. En 1999 un grupo de Los Álamos ha llegado por este procedimiento a 48 km.

De nuevo con el protocolo B92, se ha conseguido en 1998 transmitir cuánticamente clave secreta, a un ritmo de 5 kHz y a lo largo de 0,5 km en aire a plena luz del día, mediante fotones polarizados. Con esta clave Alice encriptó una foto (a razón de 8 bits por pixel), que Bob desencriptó para reconstruir la imagen primitiva, con los resultados de la figura 15[32]. En un futuro inmediato puede ser utilizado este procedimiento para generar claves secretas compartidas tierra-satélite que permitan proteger la confidencialidad de las transmisiones.

Finalmente, a finales de 1999 se ha logrado distribuir clave a lo largo de 1 km mediante un esquema variante del EPR y BB84, con pares de fotones enredados, a un ritmo de 0,4-0,8 kHz y error en los bits de un 3%. La famosa Venus «Von Willendorf»[33], debidamente digitalizada, sirvió de mensaje (figura 16)[34].

[32] Fotografía tomada del artículo de R. Hughes y J. Nordholt en *Physics World*, mayo 1999.
[33] Estatua prehistórica (24-22 ka a. C.) hallada en Willendorf (Austria) en 1908.
[34] Figura tomada de T. Jennewein, C. Simon, G. Weihs, H. Weinfurter y A. Zeilinger, http://xxx.unizar.es/archive/quant-ph/9912117.

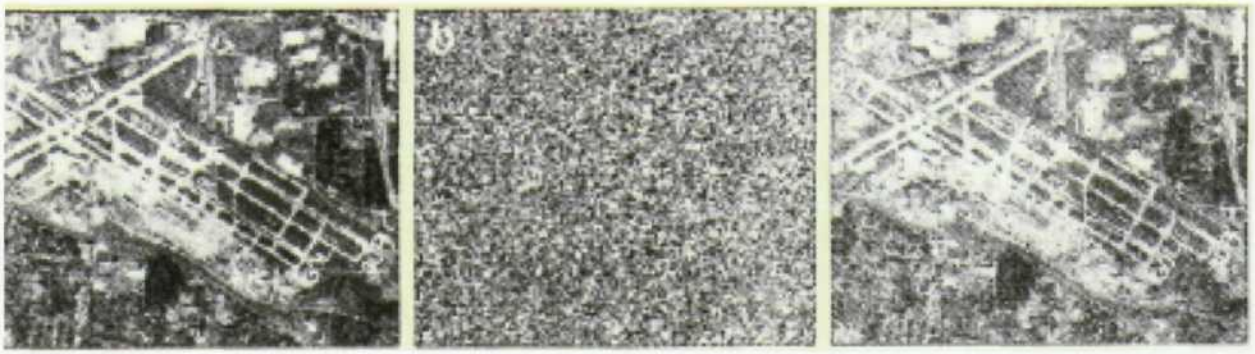

Fig. 15.– Fotografía a encriptar (izquierda). Fotografía encriptada (centro). Fotografía recobrada tras desencriptar.

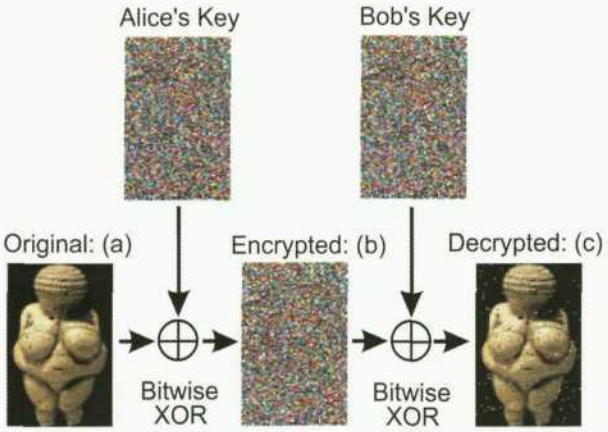

Fig. 16.– Venus a encriptar (izquierda). Mensaje encriptado (centro). Venus recobrada tras desencriptar.

QOMPUTACIÓN

Desde el modesto PC, hasta el más potente superordenador, todos los ordenadores actuales se basan en los principios de la máquina de Turing, ideada por este inglés en 1935. Pero desde hace unos pocos años se cuestiona la unicidad del modelo, y se han propuesto nuevos conceptos computacionales que van más allá de la tesis de Church-Turing según la cual todo lo «naturalmente» computable puede hacerse con una máquina de Turing y un programa adecuado. La física es la que determina qué es computable y qué no lo es.

Complejidad de los problemas

Hay tres tipos de problemas: fáciles, duros e incomputables. Fácil es, por ejemplo, ordenar alfabéticamente una lista de nombres. Duro es el problema de averiguar cómo pueden visitarse *N* ciudades conectadas por caminos unidireccionales sin pasar dos veces por la misma (el número total de ensayos a realizar crece exponencialmente con *N*). E incomputable es el problema de saber si con una colección dada de tipos de baldosas es posible o no enlosar el plano sin dejar huecos ni producir solapes; una máquina de Turing que intente resolver este problema para una colección dada puede muy bien no detenerse jamás. Surge la cuestión de si pueden existir ordenadores que «calculen lo incalculable». Y como la respuesta reside en la física, la cuestión equivale a preguntarse si existen procesos físicos no computables. De ser así, bastaría montar un ordenador «sobre la chepa» de tal proceso para tener un computador capaz de calcular algo incalculable.

La simulación de sistemas cuánticos en ordenadores clásicos es otro problema duro o intratable, según mostraron independientemente Manin y Feynman: el espacio de los estados tiene una dimensión que crece exponencialmente con el tamaño del sistema a simular.

No se sabe aún qué tipo general de problemas pueden resolverse mejor con los ordenadores cuánticos que con los clásicos. Se conocen casos particulares, como el de la factorización, o el cálculo de logaritmos discretos. Sería un gran estímulo probar que hay algún problema NP-completo[35] soluble en tiempo polinómico con un ordenador cuántico. Algunos dudan de que la eficacia de la computación cuántica llegue a tanto.

Límite cuántico a la miniaturización

Según la ley empírica de Moore, que recoge la evolución de los computadores en los últimos treinta años, cada 18 meses se duplica la velocidad de cálculo de los ordenadores y se reduce a la mitad el tamaño de los dispositivos lógicos con que los computadores almacenan y procesan información (o si se prefiere, el número de transistores en un chip clásico se multiplica por 2 cada 18 meses). A este paso, el fin de la miniaturización está muy próximo; para el año 2017 esos dispositivos lógicos alcanzarán, según la mencionada ley, tamaño atómico o molecular, y su com-

[35] Un problema *X* dícese de clase NP (polinómica no-determinista) si dada una presunta solución es posible averiguar en tiempo polinómico (en el tamaño del dato inicial) si lo es o no. Si además cualquier otro problema NP es reductible polinómicamente a *X*, dícese que *X* es NP-completo.

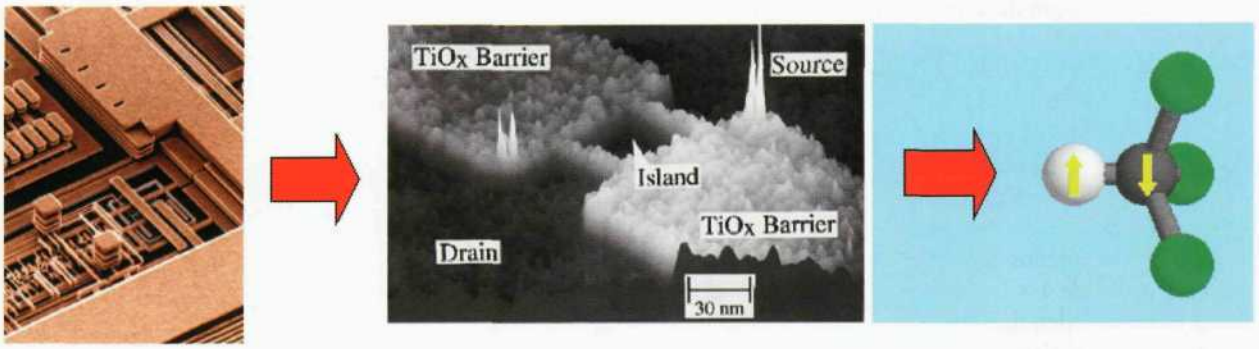

Fig. 17.– A la izquierda, chip IBM con detalles de 0,25 μm. (Los Pentium III tienen ya reglas de diseño de 0,18 μm, y se está desarrollando la tecnología de los 0,13 μm para los Pentium IV.) En el centro, un transistor monoelectrónico (SET), de tecnología nanométrica, esculpido con la punta de un microscopio de efecto túnel. A la derecha, el nivel último de miniaturización: elemento molecular de un computador cuántico, consistente en una molécula de cloroformo isotópicamente marcada, en la que los spines del átomo de H y el de ^{13}C actúan como qubits.

portamiento ostensiblemente cuántico será inevitable (figura 17) [36].

Esta barrera física a la evolución de los computadores clásicos se torna en virtud insospechada gracias a las características cuánticas. En primer lugar, los sistemas lógicos de dos estados (condensadores clásicos) dan paso a sistemas cuánticos bidimensionales, donde aparte de los estados 0 (fundamental) y 1 (excitado) poseen otros estados intermedios, que ni son 0 ni 1, sino ambos a la vez, flotando en una niebla indefinida entre estos dos valores. Esto permite que los computadores cuánticos sean mucho más eficientes en principio que los clásicos.

Puertas lógicas

En los ordenadores clásicos, las puertas lógicas que procesan la información son elementos no-lineales basados en la tecnología de los semiconductores, como los transistores, verdaderas «neuronas» del computador; en los cuánticos, las puertas lógicas se consiguen con interacciones no lineales entre las magnitudes cuánticas.

Todas las puertas clásicas tienen su contrapartida cuántica; pero hay puertas cuánticas exóticas, sin análogo clásico. Por eso toda computación clásica puede ser hecha también en un ordenador cuántico.

Una puerta monaria no clásica es $\sqrt{\text{NOT}}$, que, como su nombre indica, aplicada dos veces equivale a NOT. Es la puerta puramente cuántica que describe el efecto sobre los estados base de un sistema atómico de 2 niveles, de un pulso láser cuya duración es la mitad de la necesaria para excitar o desexcitar, y que por tanto deja al átomo en un estado indefinido, superposición de los dos estados base con amplitudes de igual módulo.

El elemento básico de un *qomputador* u ordenador cuántico es la puerta lógica CNOT: $(x, y) \rightarrow (x, x \oplus y)$ (con el símbolo $\oplus$ indicamos adición módulo 2). Cuando el input x es superposición lineal de los vectores base 0, 1, entonces el output $(x, x \oplus y)$ está enredado. El conjunto formado por todas las puertas monarias y la CNOT es universal (se bastan para simular cualquier otra puerta reversible).

Ventajas de los ordenadores cuánticos

Aunque los dispositivos semiconductores de los ordenadores clásicos deben sus propiedades a la física cuántica, éstos son clásicos en el sentido de que la información que procesan se registra en sistemas macroscópicos de 2 niveles. La diferencia entre computadores clásicos y cuánticos estriba en cómo se registra y se manipula la información, en si la base lógica es la lógica de Boole o la lógica cuántica.

El paralelismo masivo en los computadores cuánticos permite en principio una capacidad de cálculo que sobrepasa con creces las posibilidades clásicas. Con 300 qubits la dimensión del espacio de estados es $2^{300} = 2 \times 10^{90}$, y por tanto el número de operaciones en paralelo realizadas supera al número de átomos del Universo visible. Con 40 qubits el ordenador cuántico podría ya, en principio, competir favorablemente con los mayores ordenadores hoy existentes.

Los ordenadores cuánticos, teóricamente, factorizan a más velocidad, buscan en bases de datos con mayor rapidez, y simulan de modo más eficiente a los sistemas cuánticos, que los ordenadores clásicos.

Infortunios de los ordenadores cuánticos

El problema de la descoherencia es muy serio. Si T es el tiempo de relajación de 1 qubit (desexcitación), y t el

[36] La tecnología actual permite construir detalles en los microchips de tan sólo 0,25 µm. Con un orden de magnitud más pequeño, el efecto túnel podrá hacer que los electrones salten de unos hilos a otros (véase S. Benjamin y A. Ekert, en http://www.qubit.org/intros/nano/nano.html). Esto puede ocurrir ya en el 2012 *(Nature,* suplemento, diciembre 1999).

tiempo de operación de una puerta lógica, $R = T/t$ (figura de mérito) debe ser grande para que el computador funcione: ha de ser al menos del orden del (número de qubits) × (número de actuaciones de puertas). Para factorizar un número de 4 bits harían falta unas 20.000 operaciones de puertas sobre unos 20 qubits; así que R debería superar 400.000, cifra muy optimista para los modernos sistemas ópticos. Y no digamos para un número de 400 bits: R escala al menos como el (tamaño)^3, y tendría que ser R del orden de 4×10^{11}, impensable por el momento, pues con t del orden de 10^{-4} s (como en la trampa de iones del NIST), el tiempo de relajación debería superar el año[37]. Podría pensarse, para los computadores basados en trampas de iones, en aumentar la intensidad de los pulsos láser inductores de las transiciones, con el fin de disminuir t; pero esto conlleva una disminución de T, por la posibilidad de provocar transiciones no deseadas al estado excitado que por caída espontánea arruinarían la coherencia del qubit. De no remediarse el problema de la decoherencia, más allá de la factorización de un número de unos pocos bits no se podrá llegar.

Pero aunque nunca se lograra fabricar computadores cuánticos complejos, su estudio y simulación con unos cuantos bits proporcionará sin duda una visión y entendimiento más profundo de la teoría más antiintuitiva jamás descubierta por el hombre.

Ordenadores cuánticos en miniatura

El procesado de información cuántica se viene haciendo a nivel elemental desde hace medio siglo; por ejemplo, una transición estimulada entre 2 niveles es un caso de operación NOT, y una transición forzada en un sistema de 4 niveles simula la puerta XOR o CNOT.

En 1995 Cirac y Zoller[38] propusieron un método elegante e ingenioso para realizar un computador cuántico con unos cuantos qubits (de 10 a 40): iones muy fríos (temperaturas inferiores al mK) con un par de estados relevantes y de larga vida (por ejemplo, estados hiperfinos con vidas de millares de años), atrapados y dispuestos en línea en una trampa de Paul con alto vacío (10^{-8} Pa), y un láser con varios subhaces obtenidos mediante divisores y moduladores acústico-ópticos (dos subhaces incidentes sobre cada ión) con los que pueden simularse cualesquiera puestas monarias (figura 18). Para la puertas binarias se recurre a la interacción culombiana entre los iones, que provoca los modos de vibración traslacionales de la ristra iónica en el potencial de la trampa tan pronto como uno de ellos se mueve, por ejemplo bajo la acción de un haz láser.

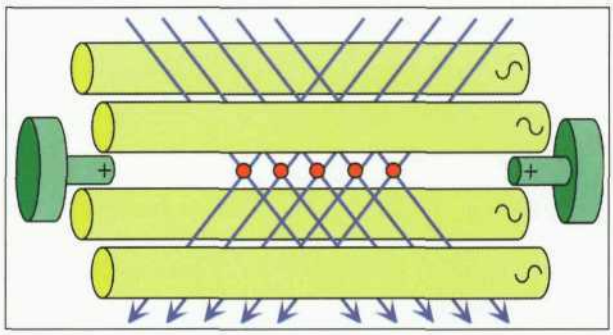

Fig. 18.– Trampa con 5 iones. La separación típica entre iones adyacentes es de unos pocos μm.

Desgraciadamente, no parece viable esta técnica para ir más allá de unas decenas de iones, por lo que su aplicación a la factorización no podrá competir con la eficacia de los ordenadores clásicos[39].

Hay otras propuestas alternativas, como la basada en RMN, en la que los qubits son estados de spin de núcleos en moléculas, manipulados mediante campos magnéticos oscilantes. En este método se manejan del orden de $O(10^{20})$ spines, y se miden polarizaciones medias del líquido que los alberga.

Algunos algoritmos cuánticos

Para explotar las potencialidades de los ordenadores cuánticos se han ideado algoritmos específicos, entre los que destacan los siguientes:

- Algoritmo XOR de Deutsch, o «cómo matar dos pájaros de un tiro».
- Algoritmo de Grover, o «cómo hallar una aguja en un pajar».
- Algoritmo de Simon, o «cómo averiguar, en tiempo polinómico en n, el período a de una función f: $\{0,1\}^n \rightarrow \{0,1\}^n$ de la que se sabe que es una función 2:1 tal que $f(x + a) = f(x)$».
- Algoritmo de Shor, o «cómo factorizar en tiempo polinómico».

Por razones de espacio y sencillez, discutiremos sólo el primero[40].

Algoritmo cuántico de Deutsch

Supongamos el siguiente problema: nos dicen que hay un oráculo que calcula una función f: $\{0,1\} \rightarrow \{0,1\}$. Se

[37] Ver el artículo de S. Haroche y J.-M. Raimond en *La Recherche*, 292, noviembre 1996.

[38] «Quantum computation with cold trapped ions», *Phys. Rev. Lett.*, 74, págs. 4091-4094, 1995.

[39] Se estima (J. Preskill, conferencia titulada *Quantum Information and Quantum Computation*, 18 mayo de 1996, en http://www.theory.caltech.edu/people/preskill/index.html) que para factorizar un número de n = 130 dígitos haría falta una trampa con 2160 iones, y habría que aplicar a este registro unos 30×10^9 pulsos láser. El número de iones crece linealmente con n, y el número de pulsos lo hace como n^3.

[40] Este algoritmo se conoce también como algoritmo de Deutsch-Jozsa. Su presentación fue mejorada por Cleve, Ekert, Macchiavello y Mosca.

trata de averiguar si la función es constante o no (es decir, es «equilibrada»), pero sólo nos permiten hacer una consulta al oráculo[41].

Clásicamente necesitaríamos consultar a éste pidiéndole $f(0)$ y $f(1)$, para comparar estos valores. Cuánticamente, sin embargo, se puede hacer de una sola tacada, con una única consulta cuántica al citado oráculo, que responde unitariamente, a saber: al presentarle un estado arbitrario $\Sigma_{ij} a_{ij} |i\rangle |j\rangle$, donde $|i\rangle$ es un estado de un primer registro de 1 qubit y $|j\rangle$ un estado de un segundo registro con otro qubit, nos devuelve $\Sigma_{ij} a_{ij} |i\rangle |j \oplus f(i)\rangle$.

Estos son los pasos del algoritmo:

1. Registros iniciales:

$$|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle$$

que no es sino el estado $|0_x\rangle|1_x\rangle$ (representando por $|0\rangle$,$|1\rangle$ los estados $|0_z\rangle|1_z\rangle$).

2. Invocación al oráculo con este estado. Su respuesta será:

$$(-1)^{f(0)}|0_x\rangle|1_x\rangle=(-1)^{f(0)}(|0\rangle|0\rangle-|0\rangle|1\rangle+|1\rangle|0\rangle-|1\rangle|1\rangle) \text{ si } f(0) = f(1)$$
$$(-1)^{f(0)}|1_x\rangle|1_x\rangle=(-1)^{f(0)}(|0\rangle|0\rangle-|0\rangle|1\rangle-|1\rangle|0\rangle+|1\rangle|1\rangle) \text{ si } f(0) \uparrow f(1)$$

3. Medida del primer registro en la base relativa al eje *Ox*. Si está en el estado $|0_x\rangle$, la función es constante; de lo contrario, es equilibrada.

Este algoritmo ha sido implementado experimentalmente mediante NMR, y muestra de modo simple e inequívoco la superioridad de los ordenadores cuánticos sobre los clásicos.

¿QUÉ SERÁ DE LA MQ EN EL SIGLO XXI?

No hay atisbos de necesidad de cambio (pero también a finales del XIX se creía terminado el edificio de la física)[42]. La MQ funciona perfectamente, diríamos que demasiado bien para los impacientes que se cansan de paradigmas ya seculares. Sólo la gravitación se resiste a la doma cuántica. La teoría de cuerdas ofrece una solución, lejana de los fenómenos a las escalas de laboratorio, y costosa en dimensiones[43]. Pero a lo mejor es el precio a pagar para una futura revolución de la física en que la propia estructura del ET se haga no conmutativa y supersimétrica, y la MQ, con su constante $\hbar$ de Planck, sea el marco obligado para expresar las nuevas dualidades que generalizan $\alpha_{EM} \leftrightarrow 1/\alpha_{EM}$. De todas formas, dado el nulo éxito de las predicciones que hace 100 años se hicieron sobre lo que iba a ser la física del siglo XX, mejor será que nos callemos, y postpongamos nuestra predicción hasta la historia que alguien contará aquí en el 2100.

Lo que sí es seguro es que, mientras tanto, los físicos experimentadores seguirán realizando brillantes exhibiciones de esas que, por ilustrar de modo simple cuestiones fundamentales de la MQ, automáticamente pasan a los libros de texto, y los físicos teóricos continuarán por un lado descubriendo resultados sorprendentemente simples (teleportación, por ejemplo) y por otro aplicando las técnicas de cálculo de la MQ a problemas cada vez más complejos, inventando procedimientos computacionales nuevos con la esperanza de que algún día se sepan hacer cálculos precisos y no perturbativos en teorías tan ricas y difíciles como la Cromodinámica Cuántica a baja energía.

BIBLIOGRAFÍA

- BROOKS, M. (pról.), *Quantum Computing and Communication,* Springer Verlag, Nueva York, 1999.
- DAVIES, P. C. W., *The New Physics,* Cambridge University Press, Cambridge, 1989.
- DEUTSCH, D., *The Fabric of Reality,* Penguin Books, Londres, 1997.
- KAHN, D., *The Codebreakers; The Comprehensive History of Secret Communication from Ancient Times to the Internet,* Scribner, Nueva York, 1996.
- MILBURN, G. J., *Schrödinger's Machines,* W. H. Freeman and Company, Nueva York, 1997.
- –, *The Feynman Processor,* Perseus Books, Reading (Massachusetts), 1998.
- INVESTIGACIÓN Y CIENCIA, *Misterios de la física cuántica,* Temas 10, 1997.
- SINGH, S., *The Code Book: The Evolution of Secrecy from Ancient Egypt to Quantum Cryptography,* Doubleday, 1999.
- TREIMAN, S. B., *The Odd Quantum,* Princeton University Press, Princeton, 1999.
- Revistas generales de física:
  – *Revista Española de Física*
  – *Physics Today*
  – *Physics World*
- Revistas de divulgación científica:
  – *Investigación y Ciencia (Scientific American)*
  – *Mundo Científico (La Recherche)*
- Direcciones de interés en la red:
  – Institut für Experimentalphysik. Universität Innsbruck. (http://info.uibk.ac.at/c/c7/c704/qo/)
  – The Physics of Quantum Information. European Research Network. (http://info.uibk.ac.at/c/c7/c704/qinet/index.html)

[41] Imaginemos, por ejemplo, que cada consulta cuesta una fortuna, o que sólo tenemos tiempo de efectuar una.

[42] Lord Kelvin llegó a decir que el futuro de la física estaba en medir hasta la sexta cifra decimal. Y Michelson, en 1894, afirmaba: *The more important fundamental laws and facts of physycal science have all been discovered ...*

[43] Tal vez la gravedad submilimétrica deje entrever pronto ese nuevo mundo.

- The Centre for Quantum Computation. Oxford University. (http://www.qubit.org/)
- Quantum Information at Los Alamos National Laboratory. (http://p23.lanl.gov/Quantum/quantum.html)
- Quantum Experiments and the Foundations of Physics. Grupo de A. Zeilinger. (http://www.quantum.univie.ac.at/)

• Archivos especializados en la red:
- LANL e-print archives (mirror) (http://xxx.unizar.es/archive/quant-ph/)