Matemáticas y sus fronteras

- BLOGS madri+d
- PORTADA BLOG
- GALERIAS IMAGENES

¿Cuánticamente seguros?

Publicado por **Matemáticas y sus fronteras** el **27 noviembre, 2016**
Comentarios (2)

Tweet

En entradas anteriores de este blog hablamos de la criptografía en su sentido más clásico, la que está basada en los números primos. Estos métodos de encriptación surgieron 1975 con W. Diffie y M. Hellman, de la Universidad de Stanford en California, quienes idearon el denominado cifrado asimétrico o clave pública. Estas claves garantizaban, por ejemplo, el anonimato de nuestros números secretos en las transferencias bancarias, en nuestro correo electrónico o cualquier pin introducido en la red.

El algoritmo, bastante seguro, se basa en la factorización de números grandes en dos números primos. Aunque el concepto sea sencillo, descubrir qué dos grandes números primos cuyo producto recupere un número de 10^{200} cifras, no es una tarea sencilla.

La denominada criptografía cuántica sustituye la teoría de números primos por las fascinantes propiedades de la teoría cuántica. Los bits clásicos de 0's y 1's del ordenador son reemplazados por qubits, or quantum bits, que no toman un valor fijo de 0 o 1, sino un estado entrelazado de estas dos posibilidades. Este estado mezcla nos recuerda a la paradoja propuesta por Schrödinger y su gato: un gato puede estar vivo y muerto a la vez. Un ordenador cuántico supone la misma paradoja, éste será capaz de realizar múltiples operaciones a la vez y afectará positivamente a nuestros actuales sistemas de privacidad. En el 2001, IBM logró desarrollar un prototipo que descomponía el número 15 en sus dos factores 3 y 5, sin embargo, la encriptación cuántica aún no ha sido propiamente desarrollada. Hasta el momento, la capacidad de factorización de un ordenador cuántico está demostrada sólo desde un enfoque teórico. Según el Washington Post, de acuerdo con los documentos que hizo

públicos el exanalista Edward Snowden, la NSA está desarrollando un robusto ordenador cuántico que es capaz de romper todos los protocolos de cifrado actuales. Incluso existen algunos productos de critografía cuántica ya en uso. En el 2010, durante el mundial de fútbol en Sudáfrica, ya se utilizaron encriptaciones cuánticas para proteger el sistema de videovigilancia del estado de Durban.

Investigadores de la Universidad de Shangai en China han anunciado el lanzamiento de un satélite de la ciencia cuántica con comunicación por el aire, que permitirá establecer redes mundiales encriptadas cuánticamente.

En el CSIC, el grupo de Criptología y Seguridad de la Información del Instituto de Tecnologías Físicas y de la Información (ITEFI), ha diseñado e implementado experimentalmente un sistema de transmisión cuántica de claves en espacio libre para entorno urbano. El sistema cuenta con un emisor, Alice, que genera los estados binarios '1' y '0' que formarán la clave criptográfica. Ambos son combinados, colimados y expandidos para ser transmitidos por el canal cuántico hasta Bob.

Emisor del sistema en espacio libre (ALICE), fuente ITEFI

La criptografía cuántica supondría un sistema de encriptación inexpugnable, el mejor sistema criptográfico posible. En esencia, para entender el procedimiento, la criptografía cuántica utiliza más la física que las matemáticas para la encriptación. Se basa en el uso de partículas luminosas, los denominados fotones de la luz y sus características. La información se almacena en el espín de un fotón. Aquí es de donde surge la analogía entre el código binario del ordenador y el espín. El espín de un fotón es 1, con tres proyecciones, la 0, 1 y -1, que dependen de su polarización. De forma sencilla, explicamos la polarización de un fotón como la oscilación de la partícula en una determinada dirección. El fotón no viaja en una línea recta, sino que se manifiesta em ondas en direcciones verticales y horizontales. La medición no se restringe sólo a estas dos direcciones, sino que puede ser una composición, y por ejemplo, ver que está oscilando en una diagonal. Por ejemplo, supongamos que tenemos una rendija vertical. El fotón atravesará esa rendija vertical si está oscilando verticalmente. Sin embargo, si oscila en diagonal, puede pasar, o no. Esta incertidumbre es el quid de la cuestión para la distribución de las claves secretas. El principio de incertidumbre restringe nuestro conocimiento de cómo supera la rendija, si en vertical, o en superposición de dos estados en diagonal, por ejemplo.

Ahora, supongamos que tenemos dos interlocutores, Alice y Bob, que deciden compartir una información. Alice envía la clave con una serie de fotones con diferentes polarizaciones, en vertical,

horizontal o un acoplamiento de estos dos estados. Esto es lo que se denomina elegir una base de estados. En el momento de la transmisión genera una cadena de qubits aleatoria y Bob recibe la cadena en otra base aleatoria. Bon recibirá el 50% de los fotones emitidos en la misma base en que Alice los emitió. Son los denominados qubits leídos que formarán la clave. Una vez generada la clave, Alice y Bob pueden usar cualquier otro canal para transmitirse los datos cifrados.

Werner Heisenberg

Si un tercer interlocutor intenta interceptar la clave, se va a producir un error al menos que el intruso siempre utilice la base de emisión de Alice. Cuando Alice y Bob compartan su base de comunicación, detectarán fácilmente si ha habido un intruso, pues obtendrán resultados muy distintos a los que esperarían en sus bases fijadas. El mensaje con la clave no se filtrará sin alterarse o destruirse, al colapsar el estado tras la medición del intruso. Este es el principio de Heisenberg de la mecánica cuántica.

Aunque parezca ciencia ficción, sin ir más lejos, este mecanismo ha sido testado en el CSIC de Madrid, que ha logrado un sistema de transmisión de claves a 300 metros de distancia con una velocidad de 1Mbit por segundo.

¿Suponen estos avances, la entrada de nuestros dispositivos a un régimen cuántico robusto, libre de fallos? La verdad es que aún se detectan errores muy ténicos para comentar en pocas líneas. Pero la línea de investigación intuye que en pocos años estaremos haciendo uso de estos métodos de encriptación de forma cotidiana y nuestras tarjetas de crédito, aunque nos roben el bolso, se hallarán a salvo de los ataques de los cacos.

———

Manuel de León (CSIC, Fundador del ICMAT, Real Academia de Ciencias, Real Academia Canaria de Ciencias, ICSU) y **Cristina Sardón** (ICMAT-CSIC).

Etiquetas:
General

Si te gustó esta entrada anímate a escribir un comentario o suscribirte al feed y obtener los

artículos futuros en tu lector de feeds.

Comentarios

Comentario by **Victor Seven** el 28 noviembre 2016 @ 11:01

Hay que destacar que este artículo da a entender algunas malinterpretaciones sobre la criptografía cuántica.

En criptografía cuántica NO se encripta ningún mensaje. De hecho, el nombre "criptografía" es incorrecto y lleva a confusión. La forma correcta de hablar de él es "distribución cuántica de claves".

Esto es porque el cifrado que se emplea es el cifrado de Vernam; este cifrado que requiere una clave secreta de la misma longitud que el texto, 100% aleatoria, compartida por receptor y emisor. Un texto cifrado con esta clave se puede demostrar matemáticamente que es imposible de descifrar.
Sin embargo, el problema es compartir la clave secreta entre emisor y receptor. Es una clave que debe ser de la misma longitud que el texto y en cada mensaje hay que usar una clave nueva para que el cifrado sea seguro. En el caso de una comunicación prolongada se nos agotarán las claves.

La distribución cuántica de claves arregla este problema. La clave se manda en forma de bits cuánticos en la forma indicada en el artículo, polarizados aleatoriamente. Cuando Alice y Bob miden con la misma rendija de polarización, la medida es correcta. En casa contrario, se descarta. Así, si Alice manda un millón de fotones, al final la clave tendrá unos 500.000 bits, puesto que acertarán al azar un 50% de las veces.
¿Qué pasa si alguien intenta espiar la comunicación? Esto se detecta rápidamente porque Alice y Bob no obtienen los resultados esperados para las medidas. Entonces se llega a la conclusión de que alguien podría conocer la clave, de forma que se desecha.
En el artículo se dice que "el mensaje no se filtrará al destruirse". Esto NO es cierto. El mensaje no se filtrará por la sencilla razón de que jamás fue enviado. Lo que se envió era una clave con la que encriptar el mensaje. Si vemos que hay alguien espiando, no podemos encriptar, no enviamos el mensaje.

Reitero: distribución cuántica de claves. Los fotones NO encriptan mensajes, se usan para que Alice y Bob se pongan de acuerdo en una clave, que posteriormente se usará para cifrar mediante Vernam.

Comentario by **Manuel** el 28 noviembre 2016 @ 11:06

¡Gracias por las puntualizaciones! Nos ayudarán sin duda a comunicar mejor este tema.

Escribe un comentario

Manuel Nombre (requerido)

mdeleon@icmat.es Correo electrónico (requerido)

URL

Tu Comentario

Enviar

Código CAPTCHA *

RSS

Buscar en el blog... IR

noviembre 2016

L	M	X	J	V	S	D
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

« oct

Contador de visitas

00579324

Archivos

- noviembre 2016
- octubre 2016
- septiembre 2016
- agosto 2016
- julio 2016
- junio 2016
- mayo 2016

- octubre 2007
- septiembre 2007
- agosto 2007
- julio 2007
- junio 2007
- mayo 2007
- abril 2007
- marzo 2007
- febrero 2007
- enero 2007
- diciembre 2006
- noviembre 2006
- octubre 2006
- septiembre 2006
- agosto 2006
- julio 2006
- junio 2006

Entradas recientes

- ¿Cuánticamente seguros?
- ¿Excelencia individual o colectiva?
- El hombre que se enfrentó a la NSA
- ¿Estamos seguros?
- Las raíces de los matemáticos
- Haciendo historia en St Andrews: MacTutor
- La física de Fermat
- Los otros teoremas de Fermat
- Lecciones de una mesa redonda
- Transferencia del conocimiento matemático

Enlaces

- DivulgaMAT
- ESTALMAT
- La Hoja Volante
- MATEMATICALIA

WEBLOGS

- :: ZTFNews.org
- Bloc de la Biblioteca de Matemàtiques
- Blog para anti-matematicos
- BUCM :: 2+2=5 :: Biblioteca Complutense
- Complejidad
- Democracia electronica
- Francis (th)E mule Science's News
- Gaussianos
- MATBUS
- Michael Trick’s Operations Research Blog

- **Páginas**
  - GALERIAS IMAGENES
- **Comentarios recientes**
  - ¿Cuánticamente seguros? | Matemáticas y sus fronteras en El hombre que se enfrentó a la NSA
  - Manuel en ¿Cuánticamente seguros?
  - Victor Seven en ¿Cuánticamente seguros?
  - ¿Cuánticamente seguros? | Matemáticas y sus fronteras en ¿Estamos seguros?
  - JOSE DAVID AREVALO COBOS en ¿Excelencia individual o colectiva?
- **Etiquetas**

  Abel Astronomía conjetura abc criptografía ecuación de quinto grado Escuela de Doctorado excelencia Formación Física estadística Johannes Kepler mochizuki Mujeres matemáticas Música Neurociencia suicidios científicos Sísifo teoría de números transferencia matemáticas
- **Acceso usuarios**

  Acceder