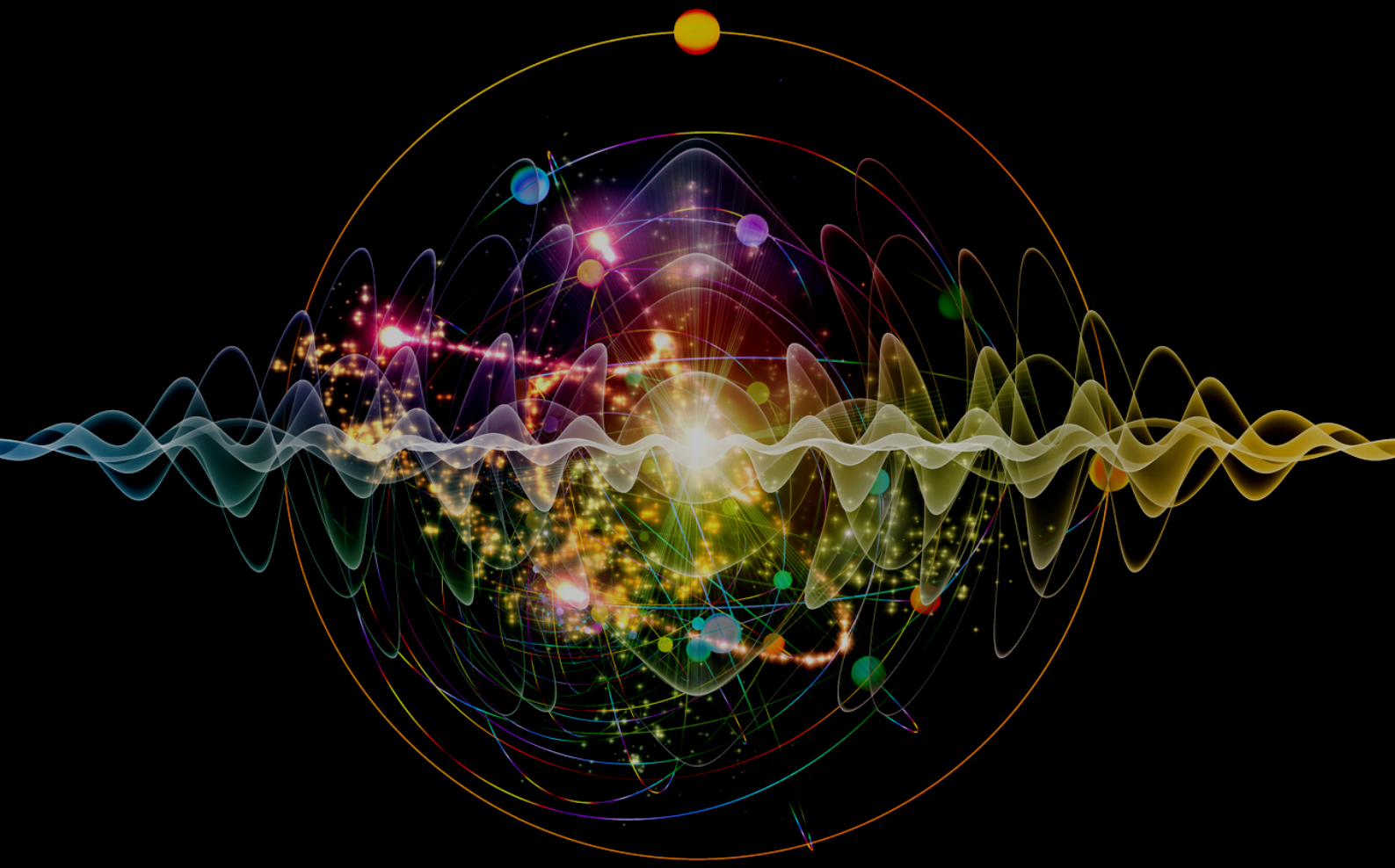
CRIPTOGRAFÍA CUÁNTICA Y SU IMPACTO EN NUESTRA CIBERSEGURIDAD



Introducción

Como introducción, empezamos definiendo la criptografía en seguridad aplicada a **proteger información**, tanto de usuarios, su información personal, particular, así como de las empresas y los gobiernos. Para ello, nos basamos en garantizar la confidencialidad, integridad y autenticidad.

Se asegura la confidencialidad con **el cifrado de las comunicaciones entre un punto y otro** protegiendo la información ante posibles amenazas de terceros en el medio de transmisión. A todo ello debería sumarse la **autenticidad e integridad** para identificar quién genera la información y que no han sido modificados.

Un buen servicio de cifrado evita esos ciberataques o engaños y, por lo tanto, nos permite vivir más seguros.

Por

Lourdes Velasco

Directora de **Cifra**
en Cipherbit-Grupo Oesía

Una amenaza presente

El concepto de criptografía cuántica ha ido cobrando cada vez más peso dentro del campo de la ciberseguridad. Este nuevo concepto va vinculado a la **aparición de los ordenadores cuánticos y los problemas que pueden conllevar a nuestra seguridad**.

La aparición de la **computación cuántica permite** resolver problemas matemáticos en un menor tiempo (criptogración clásica actual) con posibilidad de romper todas nuestras comunicaciones seguras tal y como están concebidas en la actualidad.

En la actualidad, se podrían estar almacenando todas nuestras comunicaciones, guardándose para cuando tengamos esa capacidad de cómputo cuántico para explotarlas y abrirlas. Por lo tanto, **tenemos que empezar ya a protegernos frente a estas amenazas futuras**.

¿Cómo protegernos?

Dos alternativas frente al incremento de capacidad de cómputo por los ordenadores cuánticos

Desde los algoritmos

Cambiar los actuales algoritmos matemáticos **por otros más fuertes** que no estén amenazados por una computación cuántica. Estos algoritmos ya han sido seleccionados por organizaciones internacionales, están disponibles y se están implementando y desplegando.

Desde la tecnología

Cambiar la tecnología, la forma de hacer las cosas. Y ahí es donde surge el nuevo concepto de criptografía cuántica, **aplicar la mecánica cuántica para conseguir que nuestras transmisiones sean seguras**. El termino de **criptografía cuántica es usado para identificar la tecnología de QKD (Quantum Key Distribution)**.

¿En qué consiste la criptografía cuántica?

QKD es la distribución de claves que se apoya en la mecánica cuántica. **Entre el emisor y el receptor nos enviamos fotones**. Esto hace que el medio sea seguro, porque **si alguien intenta meterse por medio a escuchar esa comunicación, los fotones son alterados** y el resultado que obtengo en el receptor es distinto, permitiéndonos percibir que la comunicación se ha comprometido.

Hasta ahora estábamos familiarizados con el concepto de bits, 0 y 1. En el caso de los fotones de lo que hablamos es de **qubits**, poniéndolos en relación con el emisor y el receptor. Donde antes podía recibir un cero o un uno **ahora puedo recibir múltiples combinaciones. El resultado de esa transmisión se usa como una clave** que, además, se inyecta en los cifradores tradicionales que protegen todas las comunicaciones, convirtiendo esa clave como **una clave secreta y segura**.

Retos de la criptografía cuántica

La criptografía cuántica está en desarrollo y conlleva muchos retos para nuestros medios actuales. Por un lado, **necesitamos poder industrializarla**, así como asegurar la interoperabilidad de equipos de distintos fabricantes, Además, requiere unos estándares de seguridad para aplicar la tecnología de forma correcta y hacer la transferencia de claves a cifradores de forma segura. Incluso tiene retos de llegar a más distancia con mejores características funcionales, proveer de más claves con independencia del medio físico.

Existen ya **iniciativas tanto en España como en otros países para cubrir distintos segmentos (terrestre y satélite)**, pero todavía debemos trabajar en cómo mejorar la tecnología para que podamos convertirla en una solución real.

Parte del éxito dependerá de poder **contar con el talento necesario** que nos permita implantar esta tecnología.

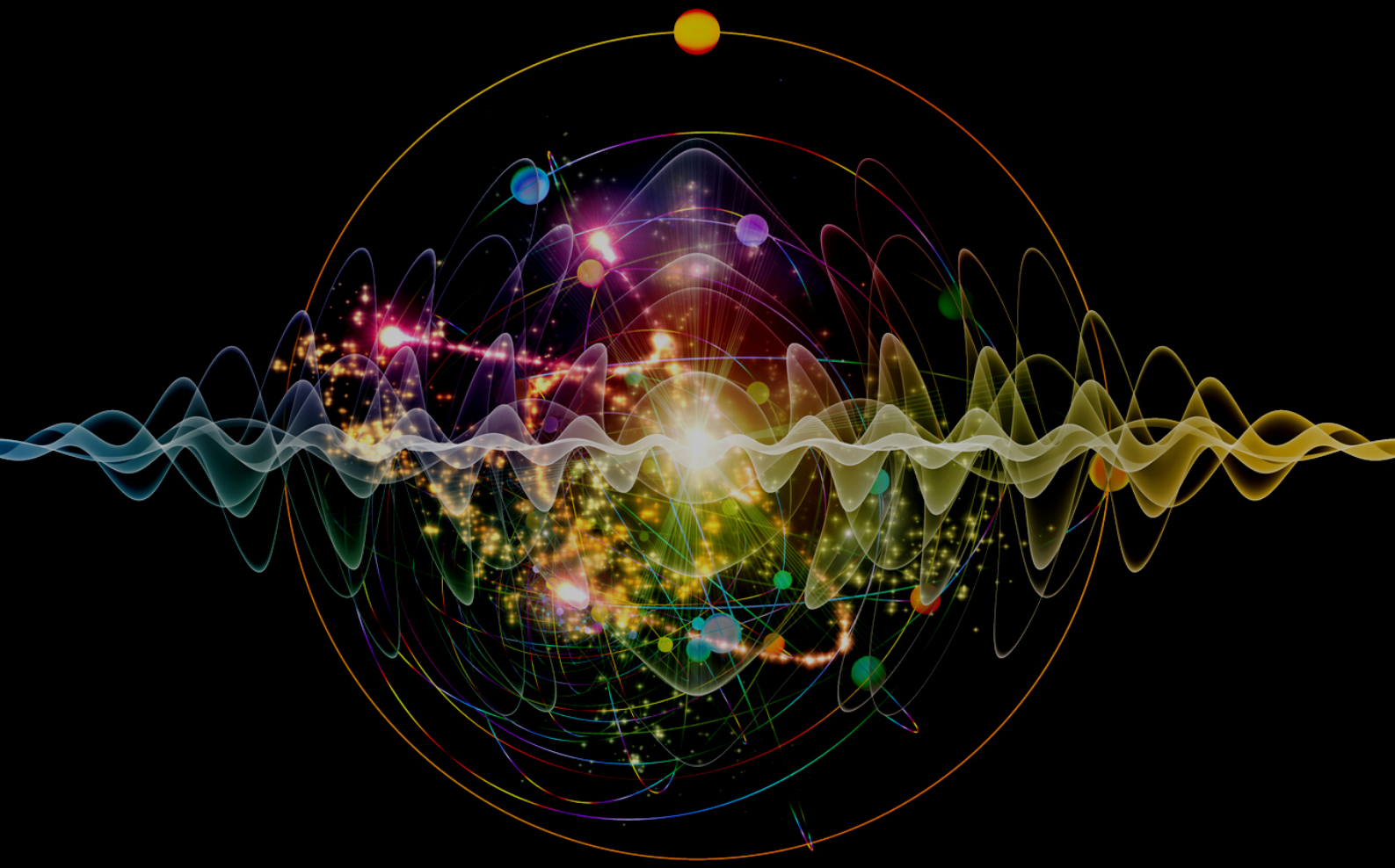
Estamos ante una nueva tecnología que **debe situar a las universidades y centros de estudios como los impulsores principales del desarrollo de estas herramientas**. Pero estas

investigaciones no deben quedarse en papers académicos para compartir en conferencias especializadas, sino que deben **dar el salto a las empresas** para poder convertirse en productos que permitan su aplicación práctica tan pronto como sea posible.

Su aplicación prioritaria debe ser el sector público, la Administración o Defensa de los Estados. Pero, hay otros tipos de **organizaciones privadas** que deben situar **cuanto antes** en su radar planes para implementar la criptografía cuántica, como es el caso de las empresas del **sector financiero**, las empresas que **gestionan instalaciones críticas** para la sociedad (como la energía), **clínicas privadas** por la información que almacenan de sus pacientes o aseguradoras que manejan información sensible de sus clientes.

En Tecnobit-Grupo Oesía nos encontramos ya trabajando en esta tecnología para contribuir con nuestra experiencia a los retos planteados: formando profesionales, estandarizando e industrializando.

oesia
grupo



Más información en: grupooesia.com/areas/ciberseguridad