

## NUEVA TÉCNICA DE DISTRIBUCIÓN DE CLAVE CUÁNTICA PARA COMUNICACIONES SEGURAS

### DESCRIPCIÓN DE LA INVENCIÓN

La revolución de las Tecnologías de la Información y la Comunicación en los últimos años ha creado la necesidad de contar con medidas de seguridad adecuadas que garanticen la protección efectiva de las comunicaciones y los derechos de los usuarios.

La invención describe un protocolo de comunicaciones para intercambiar una clave que se utiliza para cifrar información con un alto nivel de seguridad, así como el equipo que permite su implementación.

El protocolo propone la distribución de la clave cuántica basándose en la combinación de la técnica de modulación en frecuencia (FM) y la técnica de fase diferencial (DPSK). Sus características permiten conseguir mayor robustez, menor complejidad de los equipos y una mayor tasa de transferencia de clave cuántica.



### SECTORES DE APLICACIÓN EMPRESARIAL

La tecnología patentada se sitúa dentro del marco de los sistemas de comunicaciones cuánticas, y más concretamente en la distribución de claves cuánticas o criptografía cuántica (QKD). Por ello, el trabajo desarrollado por los investigadores de la UPV resulta de especial interés para la seguridad de las telecomunicaciones en aplicaciones bancarias, la transmisión de resultados electorales o las firmas electrónicas, así como en el ámbito militar y aeroespacial. En todos ellos, la seguridad de las comunicaciones resulta fundamental.

El rendimiento de este tipo de protocolos es muy bajo y por ello se reserva para establecer comunicaciones encriptadas de muy alta seguridad. Probablemente en el futuro pueda emplearse para otro tipo de comunicaciones.

### VENTAJAS TÉCNICAS Y BENEFICIOS EMPRESARIALES

La tecnología que se utiliza actualmente para este tipo de comunicaciones es el protocolo BB84. A nivel de investigación una solución es la técnica DPSK – Modulación de Fase Diferencial, cuya alta complejidad es el motivo por el que no haya sido llevada al mercado.

Las principales ventajas de la nueva técnica patentada por la UPV, respecto de BB84 son una disminución radical del grado de complejidad del receptor, que pasa a ser pasivo, una mayor tasa de transmisión, que se duplica y una mayor seguridad, que se traduce en una mayor distancia entre emisor y receptor.

Frente al esquema DPSK convencional, esta nueva técnica permite conseguir mayor estabilidad, seguridad y robustez, se tiene menor complejidad y menor coste, debido a que se utiliza un modulador como estructura interferométrica en lugar de un interferómetro óptico convencional,

El hecho de que el receptor sea más sencillo hace que la capacidad de extender esta tecnología a varios usuarios sea más competitiva, implicando una reducción de coste y su posterior mantenimiento.

## NUEVA TÉCNICA DE DISTRIBUCIÓN DE CLAVE CUÁNTICA PARA COMUNICACIONES SEGURAS

### ESTADO DE DESARROLLO DE LA TECNOLOGÍA

Además de disponer de la formulación matemática, actualmente se está trabajando en una prueba de concepto de la tecnología cuyos resultados muestran la viabilidad de la técnica a través del desarrollo de un prototipo experimental.

### DERECHOS DE PROPIEDAD INDUSTRIAL

La Universitat Politècnica de València solicitó la patente el 14 de marzo de 2012 en la Oficina Española de Patentes y Marcas. El número de solicitud que le correspondió fue el P201230385.

El proceso de internacionalización se ha iniciado mediante la solicitud del PCT, PCT/ES2013/070157.

### COLABORACIÓN BUSCADA

La Universitat Politècnica de València busca empresas interesadas en establecer acuerdos de licencia de la patente y comercializar el sistema.

### Contacto técnico

José Mora Almerich  
University Institute of Telecommunications and Multimedia Applications  
jmalmer@iteam.upv.es  
Tel. 963877000 Ext. 88143

### Contacto comercial

Elsa Domínguez Tortajada  
Centro de Transferencia de Tecnología  
eldotor@ctt.upv.es  
Tel. 963877409