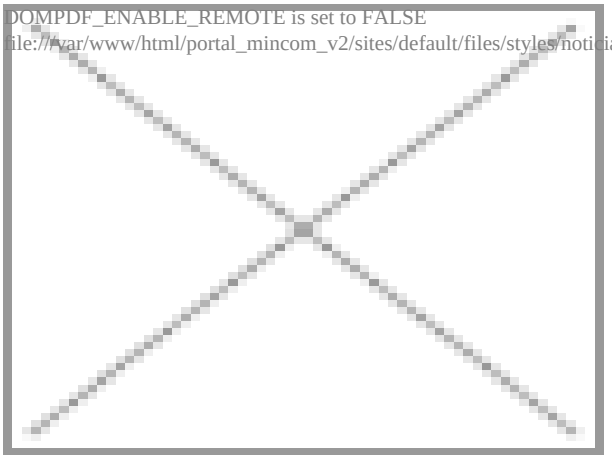

Source:
DiarioTI
El procedimiento haría posible interceptar subrepticiamente la transmisión de datos protegidos con cifrado cuántico.

El cifrado cuántico ha sido considerado la cúspide de la criptología, por tratarse de un sistema totalmente blindado y seguro, al menos en teoría. Una de sus características fundamentales es que los datos, protegidos mediante cifrado cuántico y transmitidos a través de fibra óptica, no pueden ser interceptados sin que la intrusión sea detectada por el receptor. Esto se debe a que la escucha en si modificaría las características cuánticas de los fotones recibidos.

Sin embargo, científicos adscritos a universidades suecas han demostrado que lo anterior en ningún caso es un factor absoluto. Los resultados de su investigación han sido descritos en un reciente artículo en la publicación Science Advances.

Vulnerabilidad ante ataques

Los científicos habrían aplicado un método denominado codificación de tiempo-energía, que demostraría la vulnerabilidad en cuestión: “El agujero de seguridad hace posible interceptar los datos sin ser detectados”, comenta Jan Ake Larsson, catedrático de la Universidad de Linkoping”, en un comunicado referido por la publicación. “Detectamos esta situación en nuestros cálculos teóricos, y con base en tal información nuestros colegas en Estocolmo pudieron demostrarlo en un experimento”, explica el catedrático.

El experimento en sí fue realizado por Mohamed Bourennane, catedrático dedicado a la investigación de información cuántica y óptica cuántica en la Universidad de Estocolmo. “En teoría, el cifrado cuántico funciona al 100 por ciento, pero es preciso ser cuidadosos al aplicarlo en el mundo real”, explicó Bourennane a Science Advances.

La técnica de cifrado cuya vulnerabilidad habrían comprobado los científicos se basa en un test de la conexión, realizado de manera simultánea con la generación de la clave de cifrado. El procedimiento implica la transmisión de dos fotones, exactamente al mismo tiempo, en dos direcciones opuestas. En ambos extremos de la conexión hay un interferómetro que agrega un ligero desplazamiento de fases, lo que crea una interferencia que permite comparar los datos en las dos estaciones.

Cuando el flujo de fotones es interceptado se produce ruido, que es posible detectar utilizando un teorema de la mecánica cuántica denominado desigualdades de Bell.

Si, por el contrario, la conexión es segura y carente de ruidos, los datos restantes, o fotones, pueden ser utilizados como una clave de cifrado para proteger la comunicación objeto de la transmisión.

El ataque en sí

Larsson y un grupo de estudiantes de doctorado constataron que si la fuente de fotones consiste desde una fuente lumínica tradicional, un potencial atacante puede identificar la clave, lo que en teoría le da acceso a la comunicación, sin que la intrusión sea detectada. Posteriormente, los físicos de la Universidad de Estocolmo demostraron esta teoría en la práctica, según explicó Mohamed Bourennane. Lo anterior no implica que el cifrado cuántico era “demasiado bueno para ser cierto”, o que el problema no pueda ser solucionado. En realidad, la investigación ha dejado en evidencia una vulnerabilidad dable de ser solucionada.

“Hemos propuesto varias medidas, que van desde ajustes técnicos sencillos, a una reestructuración total del proceso”, comenta la organización en su nota de prensa.

En cuanto a la utilización real del cifrado cuántico, Larsson comenta que es discutible el impacto real que su investigación pueda tener para las actuales soluciones de seguridad. Aunque las técnicas descritas están comercialmente disponibles, según el científico hay incertidumbre sobre su aplicación real: “en realidad, se trata principalmente de rumores; yo no he visto un sistema de estas características que esté siendo utilizado. Pero me consta que algunas universidades cuentan con redes de prueba para la transmisión segura de datos”, concluyó señalando Jan Ake Larsson.

Links
[1] http://diarioti.com/cientificos-vulneran-cifrado-cuantico-invulnerable/91734