Avances en distribución cuántica de claves, generación cuántica de números aleatorios y Proyecto QSI

Lic. Matías Bolaños

Resumen:

La mecánica cuántica ha probado ser una de las teorías más exitosas del siglo XX, al punto que permitió el desarrollo de nuevos avances tecnológicos, algunos de los cuales pueden poner en peligro una gran parte del sistema de encriptación global. En particular, dos de estos desarrollos tecnológicos se encuentran en un alto grado de avance, llegando incluso a nivel comercial: los algoritmos de distribución cuántica de claves (QKD) y de generación cuántica de números aleatorios. En primera instancia, QKD permite crear claves incondicionalmente seguras entre dos partes, presentando una solución a la futura crisis de encriptación. Por otro lado, los generadores cuánticos de números aleatorios (QRNG) permiten obtener aleatoriedad asegurada y certificada, sin depender de algoritmos matemáticos o fenómenos caóticos de la naturaleza.

En esta charla voy a comentar los avances más recientes en ambos campos realizados por nuestro grupo, además de presentar un proyecto novedoso que planea juntar dos campos hasta ahora separados (criptografía cuántica y criptografía post-cuántica) con la intención de desarrollar un internet seguro ante ataques realizables con computadoras cuánticas, es decir, un internet “quantum-safe”.