La aplicación de mensajería segura Signal ha anunciado una actualización en el Protocolo Signal con el fin de incorporar medidas de resistencia cuántica. Esto implica la mejora de la especificación del Triple Diffie-Hellman Extendido (X3DH) a una Diffie-Hellman Extendido Post-Cuántico (PQXDH).

> Ehren Kret de Signal comentó al respecto: *«Con esta actualización, estamos añadiendo una capa adicional de protección contra la posible amenaza de una computadora cuántica potente que, en el futuro, pueda quebrantar los estándares de cifrado actuales.»*

Este desarrollo se presenta unas semanas después de que Google incorporara soporte para algoritmos de cifrado resistentes a la computación cuántica en su navegador web Chrome y anunciara la implementación de una clave de seguridad FIDO2 resistente a la cuántica como parte de su iniciativa de claves de seguridad OpenSK el mes pasado.

El Protocolo Signal consiste en un conjunto de especificaciones criptográficas diseñadas para ofrecer cifrado de extremo a extremo (E2EE) en las comunicaciones privadas de texto y voz. Se utiliza en diversas aplicaciones de mensajería, como WhatsApp y los mensajes RCS cifrados de Google para Android.

A pesar de que las computadoras cuánticas es poco probable que se vuelvan comunes en un futuro cercano, los sistemas criptográficos actuales son vulnerables a una amenaza conocida como *«Harvest Now, Decrypt Later»* (HNDL), en la cual los datos que están cifrados hoy podrían ser descifrados en el futuro utilizando una computadora cuántica.

En otras palabras, un actor malintencionado podría robar datos sensibles cifrados de objetivos de interés y almacenarlos, lo que le permitiría aprovechar el poder de una computadora cuántica cuando esté disponible para calcular una clave privada a partir de una clave pública y desencriptar el contenido cifrado.

Para contrarrestar estas amenazas, el Instituto Nacional de Normas y Tecnología (NIST) del

Departamento de Comercio de los Estados Unidos eligió el algoritmo criptográfico post-cuántico «CRYSTALS-Kyber» para el cifrado general.

Sin embargo, en lugar de realizar una transición completa a «CRYSTALS-Kyber», la estrategia de Signal con PQXDH adopta un enfoque híbrido similar al de Google, combinando el protocolo de acuerdo de clave de curva elíptica X25519 con Kyber-1024, que apunta a ofrecer un nivel de seguridad aproximadamente equivalente al de AES-256.

> Kret explicó: *«La esencia de nuestra actualización de protocolo, desde X3DH hasta PQXDH, radica en calcular un secreto compartido, información que solo es conocida por las partes involucradas en una sesión de comunicación privada, utilizando tanto el protocolo de acuerdo de clave de curva elíptica X25519 como el mecanismo de encapsulación de clave post-cuántica CRYSTALS-Kyber.»*

> *«A continuación, combinamos estos dos secretos compartidos de manera que cualquier atacante deba comprometer tanto X25519 como CRYSTALS-Kyber para calcular el mismo secreto compartido.»*

La organización sin fines de lucro señala que el nuevo protocolo ya es compatible con las últimas versiones de las aplicaciones para clientes y tiene planes de deshabilitar X3DH para nuevos chats, requiriendo en su lugar PQXDH para todas las nuevas conversaciones *«después de un tiempo suficiente para que todos los usuarios de Signal actualicen sus aplicaciones.»*

> Signal explicó: *«PQXDH establece una clave secreta compartida entre dos partes que se autentican mutuamente basándose en claves públicas. PQXDH proporciona protección cuántica avanzada y una forma de negación criptográfica, aunque aún depende de la complejidad del problema del logaritmo discreto para la*

> *autenticación mutua en esta versión del protocolo.»*