Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Vicepresidencia Primera del Gobierno · Ministerio de Asuntos Económicos y Transformación Digital · Secretaría de Estado de Digitalización e Inteligencia Artificial
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ Instituto Nacional de Ciberseguridad

*Daniel Guerrero Villanueva*
presenta el resumen del trabajo

**Implementación del protocolo criptográfico Six-State**

*Andrea Hernández-Martín,*
*Pino Caballero-Gil y Daniel Escanez-Exposito*
Actas VIII JNIC, atlanTTic, 415-419, (2023).

24 de julio de 2024

SERIE DE RESÚMENES EN ESPAÑOL

**Palabras clave:** Criptografía cuántica, Computación cuántica, Protocolo Six-State, Qiskit

# Introducción

La computación y criptografía cuánticas están ganando rápidamente importancia gracias al respaldo de grandes empresas tecnológicas, como el procesador cuántico Osprey de IBM o el anuncio de Google del concepto de "supremacía cuántica".

Estos avances demuestran un creciente interés en las tecnologías cuánticas, por ello se han desarrollado herramientas como QuantumSolver que ofrece una interfaz web intuitiva y otra de línea de comando, facilitando el acceso a usuarios de todos los niveles.

QuantumSolver se ha enriquecido con varios algoritmos cuánticos y protocolos criptográficos. Este trabajo busca mejorar la herramienta separando algoritmos y protocolos en dos módulos: QuantumSolver Basic para algoritmos simples y QuantumSolver Crypto para protocolos de criptografía cuántica. También se ha decidido añadir un nuevo protocolo criptográfico, Six-State.

# 1. Propuesta

En el módulo QuantumSolver Basic se encuentran los algoritmos cuánticos que se han implementado en submódulos. Se puede ingresar un token de API IBM Quantum Experience o entrar como invitado. Posteriormente se elige el backend para la simulación y después el algoritmo cuántico a simular. Finalmente, se puede simular el algoritmo para ver el resultado y el circuito o hacer una simulación experimental con un histograma.

El módulo QuantumSolver Crypto cuenta con los protocolos criptográficos cuyo programa principal, de forma similar al anterior, permite elegir un portocolo y el backen a utilizar. El modo experimental está implementado de forma que junto al resultado se muestra en mapa de calor y su traza de ejecución.

# 2. Fundamento Teórico

Six-State se usa para la transmisión segura entre dos usuarios en la compuación cuántica. Este protocolo utiliza los estados proyectados en los ejes z, x e y, dados por:$\{|\mathbf{0}\rangle, |\mathbf{1}\rangle\}$, $\{|+\rangle, |-\rangle\}$ y $\{|\mathbf{i}\rangle, |-\mathbf{i}\rangle\}$.

En este algoritmo dos usuarios desean comunicarse de forma segura en un canal de comunicación cuántico unidireccional y otro clásico bidireccional, ambos públicos. El emisor genera y envía una cadena aleatoria binaria $\{|\mathbf{0}\rangle, |\mathbf{1}\rangle\}$. Después el emisor selecciona aleatoriamente una de las tres bases de medicion (eje z, eje x, eje y) para cada cúbit. Si se usa el eje z no se le aplican transformaciones. Si se elige el eje x se le aplica la puesta Hadamard: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Si se usa el eje y se le aplica una puerta creada a partir de la puerta Z y la puerta Y: $H_Y = \frac{1}{\sqrt{2}}(Y + Z) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ i & -1 \end{pmatrix}$. Después el receptor mide cada cúbit recibido de forma aleatoria entre los tres ejes. 1/3 de los cúbits serán medidos en el mismo eje que el emisor, estos se consideran correctos. Los restantes se descartan ya que al medirlos en un eje equivocado hay altas probabilidades de pérdida de información. Para realizar el descarte se hacen públicos los ejes en los que se midieron los cúbits y se eliminan los que no están medidos en el mismo eje por ambos participantes. Se comprueba la seguridad de los no descartados, si hay resultado incoherentes hay presencia de un atacante. El receptor comparte una parte de la clave recibida para que el emisor compruebe que coincide, si es así el emisor confirma que puede utilizar el resto de la clave, en caso contrario se ha lanzado un ataque eavesdropping, la clave se descarta y se reinicia el proceso.

## 3. Implementación e integración

Para la implementación se han diseñad tres entidades: Participant, Sender y Receiver; siendo la primera la principal base y las demás sus derivadas. Se comprueba la privacidad de la comunicación gracias a una libreta de un solo uso que solo comportan el emisor y el receptor.

Participant incluye métodos para generar y mostrar valores, ejes, claves y libretas de un solo uso. También crea una puerta cuántica para medir o preparar cúbits enviados respecto al eje y utilizando la clase Operator de Quiskit. La puerta se crea sumando las puertas cuánticas Y y Z, multiplicadas por $\frac{1}{\sqrt{2}}$. Para la implementación se crea un circuito cuántico y se añade la puerta necesaria.

Sender y Receiver son similares. La primera envia un mensaje para inicializar el circuito cuántico. La segunda lo recibe añadiendo la fase de medición. Hay que tener en cuenta que ambas clases utilizan la puerta cuántica vinculada al eje.

Al ejecutar QuantumSolver Crypto, se permite elegir Six-State como protocolo, se ingresa y se elige backend. Posteriormente, se puede simular el protocolo de dos maneras.

La primera permite ejecutar el algoritmos una única vez con los parámetros necesarios: un mensaje y una densidad de intercepción, que es la probabilidad con la que el receptor medirá cada cúbit. Se muestra una traza con los ejes de medición del emisor, receptor y un receptor ilegítimo con valores aleatorios entre 0 y 2 y las claves privadas. También se observa un mensaje de error si se intercepta el mensaje o un aviso de comunicación segura.

En la segunda forma, el programa se ejecuta en modo experimental, donde se simula el algoritmo varias veces, mostrando un mapa de calor que representa las condiciones de comunicación segura y las interceptaciones de las detectadas. los parámetros incluyen la longitud máxima del mensaje, la magnitud de la distancia entre densidades de intercepción y el número de repeticiones. La traza obtenida muestra los valores de los parametros y el tiempo de ejecución de las instancias restantes del protocolo.

## 4. Resultados

Se realizó un análisis comparativo de los protocolos Six-State y BB84, implementados en QuantumSolver que permite demostrar que Six-State mejora la seguridad en comparación con BB84. Los mapas de calor generados mostraron que Six-State tuvo un tiempo de ejecución similar a BB84, pero su curva fue ligeramente mejor, lo que indica una detección más efectiva de interceptores. Esto se debe a que Six-State utiliza tres estados cuánticos no ortogonales, lo que dificulta la interceptación al ofrecer información adicional sobre el estado del envio. Además, al tener tres ejes de medición en lugar de dos, reduce la probabilidad de que un interceptor mida en el mismo eje.

Los gráficos demostraron que a medida que aumenta el número de bits en el mensaje, la probabilidad de detectar al interceptor es mayor. En casos de pocos bits y alta densidad de interceptación, Six-State es más seguro ya que descarta los casos de interceptación más eficientemente que BB84.

Se observó que cuando la densidad de intercepción es cero, Six-State se considera seguro en el 100 % de los casos, lo que muestra su eficacia en entornos sin ruido. En conclusión, Six-State es más seguro que BB84 debido a su capacidad para detectar interceptores de manera más efectiva.

## 5. Discusión/Conclusiones

La librería QuantumSolver permite la ejecución de software cuántico de forma sencilla, permitiendo simular algoritmos y protocolos cuánticos con resultados visuales. Esto facilita el aprendizaje sobre criptografía y computación cuántica. Se ha presentado una propuesta de mejora en la estructura de la librería para facilitar futuras contribuciones, y se ha implementado el protocolo Six-State para distribución de claves cuánticas, demostrando su mayor fiabilidad en comparación con el protocolo BB84.

## 6. Valoración del documento original

Este documento nos muestra una interesante mejora a un herramienta que ayuda a simplificar el estudio en la computación cuántica. En un campo tan en auge siempre es importante tener en cuenta las posibles mejoras y a futuros investigadores que se esfuerzan en encontrar un nuevo método de seguir impulsando la computación cuántica.