Implementación de protocolos cuánticos de seguridad en dispositivos IoT

Raul Martinez Pavon Universidad Internacional de la Rioja, Logroño

Palabras clave: Ciberseguridad, Protocolos QKD, BB84, B92, IoT, Computación cuántica, Criptografía.

Resumen

Con el avance en todo el mundo de la digitalización, vivimos en un entorno repleto de objetos conectados a la red, desde ordenadores y móviles hasta televisiones pasando por electrodomésticos más simples. Todos estos dispositivos forman el conocido como Internet de las cosas o IoT, por sus siglas en ingles. La idea tras este trabajo es establecer un marco de referencia para la implementación de protocolos de distribución cuántica de claves, QKD, con el objetivo de hacer uso de la computación cuántica para establecer unas comunicaciones cifradas y seguras entre dispositivos. Nos enfocaremos en la implementación de estos protocolos en dispositivos de baja potencia computacional como lo son los electrodomésticos o aparatos más sencillos como enchufes inteligentes. Probaremos, por último, la eficacia de estos protocolos ejecutando ataques del tipo Man-in-the-Middle, MiTM y comprobaremos que efectivamente son protocolos que proporcionan una protección completa frente a estos ataques.

1. Introducción

El IoT es una red global de dispositivos interconectados entre si de forma directa o a través de la nube (TechTarget Contributor, 2023). Los objetos dentro de esta red del IoT, también llamados objetos inteligentes (IBM Corporation, 2023), engloban desde los más evidentes, como lo son ordenadores o teléfonos, hasta aparatos electrónicos que son, a priori, más sencillos, pero que almacenan, comparten y procesan datos, como las camaras de seguridad, o termostatos.

Sabemos desde hace mucho tiempo que cualquier dispositivo que esté conectado a la red es susceptible de convertirse en objetivo de un ataque, ya sea con el fin de robar datos o con el objetivo de controlar estos dispositivos para otro fin. Por eso, en aparatos más complejos como los ordenadores las vulnerabilidades están muy

protegidas pero en aparatos más sencillos o simplemente más económicos, la inversión en su desarrollo no es tan alta por lo que están más expuestos a ser objetos de este tipo de ataques.

Uno de los casos más mediáticos en los que se aprovecharon de una brecha de seguridad en este tipo de dispositivos es en el caso del malware, Mirai (Krebs, 2016). Mirai trataba de conectarse a dispositivos alrededor de todo el mundo para poder instalar una serie de código y hacer que estos dispositivos formaran parte de su botnet (Goel et al., 2004). De esta forma, podía controlar todos los dispositivos dentro de esta red y hacer que realicen miles de peticiones a un servidor en concreto realizando así un ataque DDoS con el fin de colapsar el servidor objetivo (Cloudflare, 2025a).

Con el crecimiento en desarrollo y utilización de este tipo de dispositivos inteligentes por un lado se han revisado este tipo de brechas de seguridad y se han tratado de mitigar al máximo, sin embargo, los ciberdelincuentes (University, 2024) han seguido buscando otro tipo de brechas para poder explotar estas vulnerabilidades en los dispositivos del IoT.

La computación cuántica puede ser especialmente útil y el uso de protocolos de distribución cuántica de claves, QKD (TechTarget, 2025) como lo son los protocolos BB84 o B92 pueden ayudar a generar claves completamente seguras para poder establecer unas comunicaciones encriptadas entre los dispositivos de forma que los ciberdelincuentes no puedan leer la información que se comparte a través de la red.

2. Estado del Arte

En todas las funciones que realiza un ordenador, la criptografía esta involucrada(IBM, 2024), necesitamos que todas las comunicaciones de cualquier tipo que realiza un dispositivo estén cifradas. Por esto mismo, actualmente se utiliza el estándar de la criptografía RSA(CertSuperior, 2024) basada en el cifrado de los mensajes mediante una clave asimétrica, es decir, la clave de cifrado y decodificación no es la misma, aunque están relacionadas por diversos procesos matemáticos. La seguridad de estas claves se basa en el problema de la descomposición en factores primos. Estas claves tienen una longitud de unos 2000 bits, por esto mismo, los computadores actuales no son capaces de romper estos protocolos dado que tardarían siglos en realizar los cálculos necesarios. Sin embargo, la computación cuántica y algoritmos como el de Shor (1994) pueden realizar estos cálculos en una cantidad de tiempo razonable, por lo que todos estos sistemas vuelven a ser completamente vulnerables.

Para proteger la información podemos emplear distintos protocolos para generar las

claves haciendo uso de la computación cuántica, como el protocolo B92 (Bennett, 1992), por lo que la seguridad no dependerá de la complejidad matemática del encriptado, sino de la naturaleza misma de la información.

2.1. Protocolo B92

El protocolo B92 nace como mejora del protocolo original de uno de sus creadores como mejora del algoritmo original, BB84 (Bennett & Brassard, 1984), simplificando la ejecución del mismo. Los dos interlocutores, Alice y Bob, podrán generar una clave completamente segura a traves del envio de cúbits codificados en dos estados no ortogonales, como lo son el estado $|0\rangle$ y el $|+\rangle$, (Guillén & Gasca, 2006).

Primero Alice generará una clave inicial, una serie de bits aleatorios de una longitud acordada inicialmente. Tras esto codificará y enviará a Bob una serie de cúbits a través del canal cuántico siguiendo la siguiente regla: Si el bit original es un 0 se enviará el estado$|0\rangle$ mientras que si el bit original es un 1, Alice, enviará el estado $|+\rangle$.

De esta forma Bob recibirá los cúbits y los medirá eligiendo aleatoriamente una Base para medir el cúbit entre el eje X y el eje Z. Si Bob elige el eje Z y obtiene un resultado de 0, el cúbit original podría estar en $|0\rangle$ o haber colapsado desde el estado $|+\rangle$, mientras que si mide 1, este resultado solo ha podido venir del colapso del estado $|+\rangle$, por lo que el bit original era un 1. De la misma forma, si Bob elige el eje X y mide un 0, el cúbit podría estar en $|+\rangle$ o haber colapsado desde el estado $|0\rangle$, mientras que si mide 1, este solo podría haber resultado del colapso del estado $|0\rangle$ por lo que el bit original era un 0.

Siguiendo esta lógica Bob construirá una nueva clave binaria y guardará las posiciones de los cúbits de los que ha podido medir el resultado 1. Esta lista de índices al igual que una parte de la clave nueva la enviará a Alice. Ahora, Alice, tomará de la clave original solo los bits según las posiciones que le ha comunicado Bob y comparará esta nueva clave con la clave de control que le ha enviado Bob. Si ambas claves de control coinciden la clave generada es completamente segura. En caso de la existencia de un atacante, Eve, las claves de control no coincidirán dado que, Eve, al intentar leer los cúbits ha modificado su estado y provocado el colapso de ellos dejando huella.

3. Simulaciones realizadas

3.1. Ejecución del protocolo B92 y ataque MiTM

Para poder crear las simulaciones para comprobar si el protocolo B92 es realmente efectivo, se ha utilizado dos Raspberry Pi modelo 3B (Raspberry Pi Foundation, 2016) a las que hemos instalado un sistema operativo

basado en la distribución Debian de Linux (Raspberry Pi Foundation, 2025a), (Raspberry Pi Foundation, 2025b).

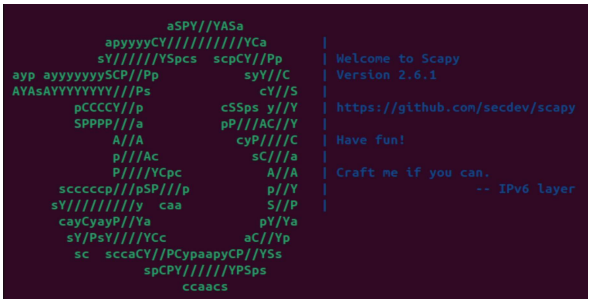
Además, se ha necesitado instalar los paquetes de qiskit (IBM Quantum, 2025) y qiskit-aer (Qiskit Development Team, 2025) para poder simular la codificación y lectura de los cúbits involucrados. La conexión entre las dos Raspberrys, que llamaremos Alice y Bob, se ha realizado mediante el paquete socket de python, que nos permite realizar conexiones y comunicaciones entre dispositivos de una misma red LAN (Cloudflare, 2025b). Abriremos el puerto 2220 de en la dirección IP local de Alice para que Bob pueda realizar la conexión.

Una vez hemos realizado la conexión podremos ejecutar el protocolo B92 siguiendo los pasos ya comentados obteniendo un archivo de texto en cada uno de los dispositivos de Alice y Bob en el que hemos guardado las claves finales para, de este momento en adelante, poder cifrar las comunicaciones entre ellos.

Tras probar que el protocolo se ejecuta correctamente hemos realizado una simulación de un ataque MiTM (Keeper Security, Inc., 2023) para crear la presencia de Eve como posible atacante en la red. Para ello se ha utilizado una máquina virtual haciendo uso de la aplicación VirtualBox (Oracle Corporation, 2023) instalando el sistema operativo Ubuntu (Canonical Ltd., 2023), creando un sistema de laboratorio aislado del sistema Windows 11 anfitrión. Además hemos necesitado instalar los paquetes de qiskit y qiskit-aer para poder realizar las simulaciones cuánticas necesarias, así como el paquete Scapy (Biondi et al., 2023) que hemos utilizado para interceptar los paquetes de información que circulan por la red entre Alice y Bob.

Tras ejecutar primeramente el protocolo,

Figura 1: *Paquete Scapy en la terminal de Ubuntu en VirtualBox*



hemos podido obtener una clave guardada en el archivo key.txt que, al no haber presencia de ningún atacante ambas claves coinciden a la perfección por lo que las comunicaciones podrían cifrarse sin problema.

Sin embargo, en el momento que ejecutamos el script de Eve como atacante, por lo que estamos tratando de leer los cúbits que circulan entre Alice y Bob, y por tanto, los estamos manipulando, las claves final y original no coinciden por lo que el protocolo nos alerta que el canal de comunicación ha sido comprometido y se debe reiniciar el protocolo hasta poder crear una clave que sí sea

Figura 2: *Comunicación establecida sin presencia de atacante.*

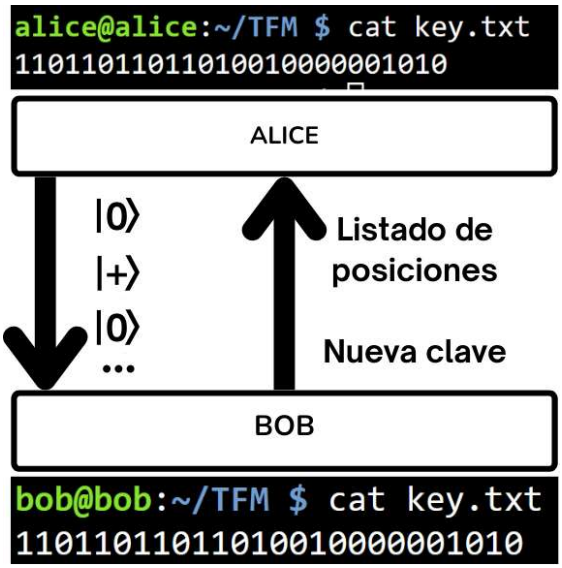
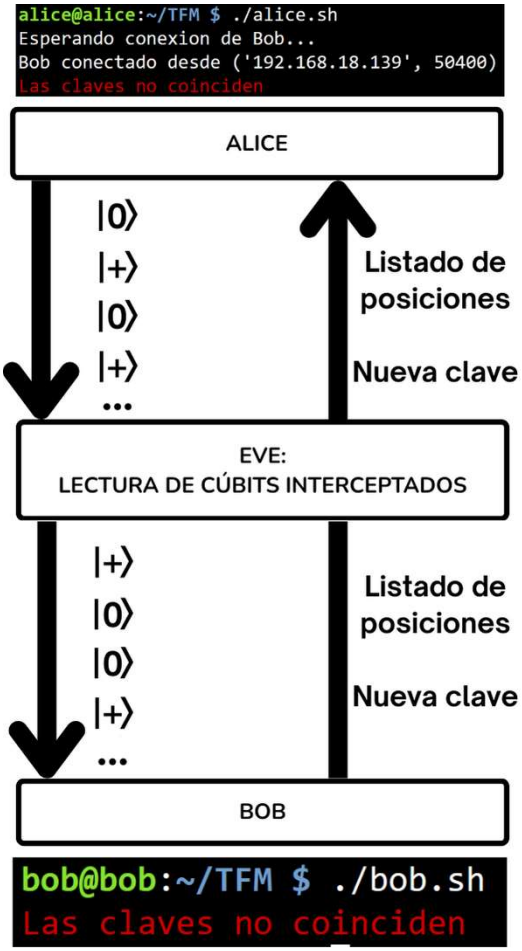


Figura 3: *Comunicación establecida con la presencia de Eve.*



segura y no haya sido interceptada por ningún atacante.

3.2. Implementación física de una red cuántica

Para poder implementar este tipo de tecnologías para proteger nuestra privacidad del día a día necesitamos incluir en nuestras redes dos factores imprescindibles. Por un lado necesitamos una serie de procesadores que sean capaces de poder generar, codificar, enviar, recibir y medir los cúbits codificados para poder establecer la clave secreta para el cifrado. En la actualidad existen soluciones como el Sceptre-Duo de HEQA-Sec (2024) que son capaces de realizar estas tareas. Sin embargo, las soluciones actuales, por tamaño y recursos necesarios para su utilización están diseñados y fabricados para ser implementados en la industria, en centros de datos o centros de servidores donde el tamaño y la potencia necesaria no es un impedimento. Sin embargo, para poder implementar este tipo de protocolos en la tecnología de consumo, para usuarios promedios se requiere poder reducir sobre todo, el tamaño de los procesadores cuánticos.

Por otro lado, es necesario la instalación de una red cuántica, un medio por el que poder propagar los cúbits de un dispositivo como

Alice a otro dispositivo como Bob. La solución actual más prometedora es la computación cuántica con fotones. Este tipo de cúbits tienen dos ventajas principales, por un lado no requieren temperaturas criogénicas como otros tipos por lo que son ideales para entornos no controlados como los domicilios de los usuarios. Además la instalación actual de fibra óptica de internet es aprovechable para realizar la transmisión de cúbits entre dispositivos.

Sin embargo, para que se pueda hacer efectiva realmente la implementación de estas tecnologías en la vida diaria es necesario, principalmente, solucionar los diferentes desafíos actuales de la computación cuántica en relación a la decoherencia y los algoritmos de detección de errores. Por otro lado, es también necesaria una educación a nivel social en torno a este tipo de dispositivos dado que el desconocimiento de la población puede provocar el rechazo de estas tecnologías que, como hemos visto, pueden ser de gran utilidad para poder proteger los datos de carácter privado.

4. Conclusiones

Hemos podido ver la gran importancia de la computación cuántica así como la implementación de protocolo cuánticos de seguridad en el ámbito de la ciberseguridad y la información actual. La seguridad informática actual se basa en complejos problemas matemáticos que un ordenador moderno no puede resolver, sin embargo un ordenador cuántico puede romper este tipo de barreras de seguridad pudiendo así ganar acceso a toda la información de la red. Aun así, hemos visto que al igual que la computación cuántica es un problema para la seguridad informática de hoy, también es su solución. Hemos visto cómo el uso de protocolos cuánticos de seguridad como lo es B92 proporcionan una barrera que no se basa en la complejidad del protocolo sino que es la naturaleza misma de los cúbits la que proporciona la seguridad a las claves que se generan haciendo uso de estos algoritmos.

Hemos visto a través de las simulaciones cómo, efectivamente, estos protocolos de seguridad son realmente efectivos contra los ataque del tipo MiTM dado que una simple comparación entre la información enviada y recibida asegura completamente a los interlocutores que si la información coincide es una confirmación definitiva que el canal de comunicación es completamente seguro ya que si estuviera mínimamente comprometido la información recibida seria totalmente diferente por lo que el intruso es fácilmente detectable.

Además hemos podido indagar en la posibilidad actual de poder implementar físicamente estos sistemas de criptografía cuántica y, aunque, a día de hoy, estos dispositivos es-

tán pensados para ser instalados en centros de datos e instalaciones similares, el desarrollo continuo de estos instrumentos permite que en un futuro, si se ha podido reducir el tamaño de los procesadores, como característica principal, puedan ser implementados dentro de dispositivos de consumo como ordenadores actuales, u objetos inteligentes como electrodomésticos modernos.

Referencias

Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 3121-3124.

Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*.

Biondi, P., et al. (2023). *Scapy: the Python-based interactive packet manipulation program & library*. Consultado el 4 de agosto de 2025, desde https://scapy.net/

Canonical Ltd. (2023). *Download Ubuntu Desktop*. Consultado el 1 de septiembre de 2025, desde https://ubuntu.com/download

CertSuperior. (2024). *¿Qué es la criptografía RSA?* Consultado el 7 de mayo de 2025, desde https://www.certsuperior.com/que-es-la-criptografia-rsa/

Cloudflare. (2025a). *¿Qué es un ataque DDoS?* [Centro de aprendizaje de Cloudflare]. Consultado el 21 de abril de 2025, desde https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/

Cloudflare. (2025b). *¿Qué es una LAN (red de área local)?* Consultado el 16 de junio de 2025, desde https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-lan/

Goel, S., Baykal, A., & Pon, D. (2004). Botnets: The Anatomy of a Case. En *Security in the Information Society: Visions and Perspectives*. University at Albany, Center for Information Forensics; Assurance.

Guillén, E. P., & Gasca, J. J. N. (2006). Ciencia e Ingeniería Neogranadina. Universidad Militar Nueva Granada.

HEQA-Sec. (2024). *Sceptre-Duo*. Consultado el 15 de mayo de 2024, desde https://heqa-sec.com/sceptre-duo/

IBM. (2024). *¿Qué es la criptografía cuántica segura?* Consultado el 7 de mayo de 2025, desde https://www.ibm.com/es-es/topics/quantum-safe-cryptography

IBM Corporation. (2023). *What is the Internet of Things (IoT)?* IBM. Consultado el 20 de abril de 2025, desde https://www.ibm.com/think/topics/internet-of-things

IBM Quantum. (2025). *Qiskit: Open-source quantum computing software*. Consultado el 18 de mayo de 2025, desde https://www.ibm.com/quantum/qiskit

Keeper Security, Inc. (2023). *Man-in-the-Middle Attacks (MITM)*. Consultado el 2 de agosto de 2025, desde https://www.keepersecurity.com/es_ES/threats/man-in-the-middle-attacks-mitm.html

Krebs, B. (2016). *New Mirai Worm Knocks 900K Germans Offline*. Krebs on Security. Consultado el 20 de abril de 2025, desde https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/

Oracle Corporation. (2023). *Oracle VM VirtualBox*. Consultado el 1 de septiembre de 2025, desde https://www.virtualbox.org/

Qiskit Development Team. (2025). *Qiskit Aer: High performance quantum computing simulation*. Consultado el 18 de mayo de 2025, desde https://qiskit.github.io/qiskit-aer/

Raspberry Pi Foundation. (2016). *Raspberry Pi 3 Model B*. Consultado el 18 de mayo de 2025, desde https://www.raspberrypi.com/products/raspberry-pi-3-model-b/

Raspberry Pi Foundation. (2025a). *Raspberry Pi OS - The official operating system for all models of the Raspberry Pi*. Consultado el 5 de septiembre de 2025, desde https://www.raspberrypi.com/software/operating-systems/

Raspberry Pi Foundation. (2025b). *Raspberry Pi OS – Operating System*. Consultado el 18 de mayo de 2025, desde https://www.raspberrypi.com/software/

Shor, P. W. Algorithms for Quantum Computation: Discrete Loragithms and Factoring. En: En *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994.

TechTarget. (2025). *Quantum key distribution (QKD)*. Consultado el 14 de junio de 2025, desde https://www.techtarget.com/searchsecurity/definition/quantum-key-distribution-QKD

TechTarget Contributor. (2023). *Internet of Things (IoT)*. TechTarget. Consultado el 20 de abril de 2025, desde https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

University, M. (2024). *¿Qué es un ciberdelincuente?* Consultado el 7 de mayo de 2025, desde https://msmk.university/ciberdelincuente/