Grado en Gestión de Ciberseguridad

Año académico 2023 / 2024

2024

Computación cuántica aplicada a la criptografía

Jaime Navarro

Universidad Francisco de Vitoria

12-6-2024

DECLARACIÓN PERSONAL DE NO PLAGIO

Yo, Don…….Jaime Navarro con NIF/NIE…. id removed for security reasons …. estudiante del **Grado Gestión de la Ciberseguridad** de la Universidad de Francisco de Vitoria, como autor/a de este documento académico, titulado Computación cuántica aplicada a la criptografía, presentado como **Trabajo de Fin de Grado**, para la obtención del Título correspondiente, **declaro que, es fruto de mi trabajo personal, que no copio, que no utilizo ideas, formulaciones, citas integrales e ilustraciones diversas, sacadas de cualquier obra, artículo, memoria, etc., (en versión impresa o electrónica), sin mencionar de forma clara y estricta su origen, tanto en el cuerpo del texto como en la bibliografía**.

Así mismo, soy plenamente consciente de que el hecho de no respetar estos extremos es objeto de sanciones universitarias y/o de otro orden.

En…… Madrid, a…. *12* de…….. *Mayo* de…… *2024*

Fdo. sign removed for security reasons

(*firma*)

Índice

Introducción e historia

Este trabajo final de Grado trata sobre la computación cuántica y su aplicación en la criptografía. Empezando por el "estado del arte", el grado de maduración y viabilidad que tiene la computación cuántica. Esta sería una línea del tiempo muy completa de los acontecimientos relevantes para la computación cuántica, con todas sus fuentes:

"Descubrimiento de la Teoría Cuántica: A principios del siglo XX, científicos como Max Planck y Albert Einstein revolucionaron nuestra comprensión de la física al proponer que la energía se emite y absorbe en pequeñas unidades llamadas "cuantos". Estos descubrimientos sentaron las bases de la teoría cuántica y allanaron el camino para el desarrollo de la computación cuántica". [1]

1970 - James Park publicó el teorema de Imposibilidad de un esquema de medición no perturbador simple y perfecto, que después influiría en 1982 en el teorema de no clonación, que explica la imposibilidad de una copia independiente e idéntica de un estado cuántico arbitrario desconocido. [2]

En otras palabras, no se puede "leer" el estado cuántico, y saber si es "1" o "0" porque al leer, alteramos su estado. [2] Referencia: [ACM SIGACT News, Volume 15, Issue 1. pp 78–88]

1980: Paul Benioff es conocido por ser el primero en aplicar la teoría cuántica a los sistemas de computación. [3]

- Propuso un modelo mecánico cuántico de la máquina de Turing. Téngase cuidado de no confundir esta máquina de Turing con la máquina de bombeo que diseñaron un grupo de

criptoanalistas británicos liderados por Alan Turing. La máquina de Turing, que éste propuso en 1936 es un modelo teórico de computación y comunicación. Pero sólo teórico. [4]

-1980: “Yuri Manin expressed the revolutionary idea of Quantum Computing and Quantum Information before Richard Feynman did” , en otras palabras, Yuri Manin, planteó antes que Richard Feynman la posibilidad del procesador con “c” elevado a “N” estados [5] , además del clásico bit “0” o “1”,en “Max Planck Institute for Mathematics”, Bonn, Alemania, a pesar de que empezó sus estudios en la Unión Soviética, cuando ésta tuvo que . [6]

- 1981: Richard Feynman

- Feynman propuso un dispositivo llamado "computadora cuántica" para aprovechar las leyes de la física cuántica para lograr aceleraciones computacionales sobre los métodos clásicos. [7]

- Feynman y Yuri Manin sugirieron que una computadora cuántica tenía el potencial de simular cosas que una computadora clásica no podría hacer factiblemente. [8]

-1984: Charles H. Bennet y Gilles Brassard:

-Ambos proponen el primer QKD (Quantum Key Distribution), en español, sistema de distribución de claves cuánticas, conocido como “BB84”. [63]

-1985: David Deutsch [9]

- David Deutsch fue pionero en el campo de la computación cuántica, siendo el primero en formular un algoritmo cuántico. [10]

- Su trabajo en 1985 allanó el camino para las rudimentarias computadoras cuánticas en las que los científicos están trabajando hoy. [11] también colaboró con Gilles Brassard, quien desarrolló criptografía resistente a la computación cuántica [12]

- 1993: Dan Simon [13]

- Dan Simon es conocido por el algoritmo de Simon, que proporcionó el primer ejemplo de una aceleración exponencial sobre el mejor algoritmo clásico conocido al usar una computadora cuántica para resolver un problema particular. [14]

- Simon presentó su algoritmo en 1993, pero fue rechazado inicialmente. Sin embargo, Peter Shor, que estaba en el comité del programa de esa conferencia, vio el potencial del algoritmo de Simon y trabajó en su propio algoritmo, que se convirtió en el famoso algoritmo de Shor.

- 1993: Charles Bennett

Colaboró con Gilles Brassard para desarrollar el esquema criptográfico cuántico que se basa en enredos qubits, cuyo protocolo "BB84" [15] se usó para la transmisión segura de datos a lo largo de redes ópticas [16] e incluso vía satélite a más de miles de kilómetros. [17] [18]

- Charles H. Bennett es conocido por su trabajo en la física de la información, aplicando la física cuántica a los problemas que rodean el intercambio de información.

- Bennet y Brassard han jugado un papel importante en la explicación de las interconexiones entre la física y la información digitalizada, particularmente en el ámbito de la computación cuántica. Bennet con Brassard: [19]

- 1995: Peter Shor [20]

- Peter Shor es conocido por su trabajo en la computación cuántica, en particular por idear el algoritmo de Shor, un algoritmo cuántico para factorizar exponencialmente más rápido que el mejor algoritmo conocido que se ejecuta en una computadora clásica. [21]

- El algoritmo de Shor es uno de los pocos algoritmos cuánticos conocidos con aplicaciones potenciales convincentes y fuertes evidencias de aceleración "superpolinomial" en comparación con los algoritmos clásicos. [22]

- 1996: Lov Grover [23]

- Lov Grover es conocido por ser el originador del algoritmo de búsqueda de base de datos Grover utilizado en la computación cuántica.

- El algoritmo de Grover de 1996 ganó renombre como el segundo algoritmo importante propuesto para la computación cuántica (después del algoritmo de Shor de 1994) y en 2017 finalmente se implementó en un sistema cuántico físico escalable [24]

Un proyecto realizado en la Escuela Colombiana de Ingeniería Julio Garavito estudió el estado del arte en computación cuántica, exploró a profundidad los algoritmos de Grover y Shor, y realizó implementaciones y extensiones de dichos algoritmos en el computador cuántico de IBM1. Las contribuciones concretas de este proyecto fueron material didáctico para la enseñanza de Computación Cuántica, un documento que describe el estado del arte, y los algoritmos de Grover y Shor, y finalmente las implementaciones de los algoritmos en la máquina de IBM. [24]

- 1997: Primeros experimentos [25]

- A finales de la década de 1990 y principios de la década de 2000 se realizaron varios hitos experimentales.

- En 1998, se demostró la primera computadora cuántica de 2 qubits por un grupo en IBM. Fue presentada en Universidad de Berkeley, California, Estados Unidos. “In 1998 Isaac Chuang of the Los Alamos National Laboratory, Neil Gershenfeld of the Massachusetts Institute of Technology (MIT), and Mark Kubinec of the University of California at Berkeley created the first quantum computer (2-qubit) that could be loaded with data and output a solution.” [26]

- 1998: Primeros qubits

- En 2023, se logró operar qubits a temperaturas algo más altas, un paso clave hacia la simplificación de los requisitos del sistema, dado que estos qubits suelen operar, o mejor dicho se les hace operar a temperaturas por debajo de -200 grados Celsius. Son temperaturas ultra bajas usadas para mejorar la estabilidad en su funcionamiento. En Azure quantum, una división de Microsoft, buscan “diseñar y fabricar dispositivos con

precisión de nivel atómico" superponiendo materiales semiconductores y superconductores. [27]

- Se utilizó una única molécula como qubits por primera vez. [28]

- 2000: Progreso de Qubits

- IBM presentó su procesador Osprey de 433 qubits en 2021 y tiene como objetivo lanzar un procesador de 1,121 qubits llamado Condor en 2023. [29]

- En 2023, IBM también presentará su procesador Heron, que tendrá solo 133 qubits. Aunque puede parecer un paso atrás, los qubits de Heron serán de la más alta calidad y cada chip podrá conectarse directamente con otros procesadores Heron. [30]

Existe un artículo que recopila de forma muy completa los hitos más relevantes de los años 80 y 90 especialmente, en la computación cuántica: en los 80 del siglo pasado, Yuri Manin con su libro en ruso "Computable and Uncomputable" la idea de un autómata cuántico que utilizara la superposición y el entrelazamiento, Paul Benioff con un modelo mecánico cuántico hamiltoniano microscópico de ordenadores representados por máquinas de Turing, entre otros hitos. [31]

Estado del arte actual en computación cuántica, y hacia dónde vamos

Estado del arte actual:

Las tecnologías cuánticas están en rápido desarrollo y podrían suponer una amenaza significativa para la criptografía actual basada en algoritmos como RSA y ECDSA.

La criptografía post-cuántica es un campo de investigación que busca desarrollar nuevos algoritmos y protocolos criptográficos resistentes a ataques cuánticos.

Actualmente, no existe una solución única y definitiva para la criptografía post-cuántica. Se están investigando y desarrollando diversas propuestas, pero aún no hay un estándar claro.

Riesgos de la criptografía actual:

Los ataques cuánticos podrían romper la confidencialidad e integridad de las comunicaciones protegidas por la criptografía actual.

Esto podría tener graves consecuencias para la seguridad nacional, la privacidad individual y la economía digital.

Se estima que los ataques cuánticos podrían ser viables en la próxima década.

Cifrados y usos:

- La criptografía actual se utiliza para proteger una amplia gama de datos y comunicaciones, incluyendo:
    - **Transacciones financieras**
    - **Comunicaciones gubernamentales y militares**
    - **Registros médicos**
    - **Datos de identidad**
    - **Infraestructuras críticas**

Objetivos clave de Europa:

- El **documento de la EPC** (European Policy Centre) establece una serie de objetivos clave para la criptografía post-cuántica en Europa:

- **Desarrollar y adoptar estándares de criptografía post-cuántica.**
- **Invertir en investigación y desarrollo en esta área.**
- **Aumentar la sensibilización sobre los riesgos de la criptografía actual.**
- **Preparar a las organizaciones públicas y privadas para la transición a la criptografía post-cuántica.**
- **Cooperar con otros países y organizaciones internacionales.**

Fecha límite:

- El documento de la EPC establece una fecha límite de **2024** para que las organizaciones europeas comiencen a **planificar la transición a la criptografía post-cuántica**.
- Se espera que la **adopción generalizada** de la criptografía post-cuántica se produzca en la próxima década.

  - **Algoritmos basados en redes**
  - **Algoritmos basados en códigos**
  - **Algoritmos basados en firmas multivariadas**

Comparación entre Europa y Estados Unidos:

- Tanto Europa como Estados Unidos están **invirtiendo en investigación y desarrollo** de la criptografía post-cuántica.
- Sin embargo, hay algunas **diferencias clave** en sus enfoques:
  - **Europa** está adoptando un enfoque más **colaborativo** y está trabajando para desarrollar estándares abiertos.
  - **Estados Unidos** está adoptando un enfoque más **competitivo** y está permitiendo que el mercado desarrolle soluciones.

En otras palabras:

- La criptografía post-cuántica será un **tema complejo y crucial** para la seguridad nacional y la economía digital. Todos confiamos en cifrados como lo pueden ser AES 128 bits cuando hacemos una compra en internet con tarjeta, hacemos transferencias bancarias desde nuestros dispositivos en una aplicación o la web. O sin ir tan lejos, las casas en las que vivimos. ¿quién certifica que la casa es nuestra? La casa que prácticamente toda la población trabaja durante más de 20 años para pagarla. Esto reside en certificados electrónicos, cuya criptografía no sabemos si el día del mañana en un plazo de 10 años o poco más sigan siendo seguros.

Es importante que tanto Europa como Estados Unidos continúen **invirtiendo en investigación y desarrollo** en esta área y que trabajen juntos para desarrollar **soluciones seguras y escalables**.

Documento de la EPC sobre criptografía post-cuántica [32]

Sitio web del NIST sobre criptografía post-cuántica [33]

Artículo sobre criptografía post-cuántica [34]

Con referencias del documento y con las anteriores afirmaciones, las que sí menciona dicho PDF [35]

Hacia dónde vamos. Los ordenadores de IBM en los próximos 10 años

El artículo de Technology Review expone el ambicioso proyecto de IBM para desarrollar un ordenador cuántico a gran escala con 100.000 qubits. Este hito tecnológico promete revolucionar diversos campos, desde la medicina y la ciencia de materiales hasta la inteligencia artificial y la seguridad informática. Algunas ideas clave:

Escalabilidad: IBM busca superar las limitaciones actuales de los ordenadores cuánticos, aumentando drásticamente el número de qubits, la unidad fundamental de información cuántica, con “0”, “1” y el estado superpuesto de ambos.

Arquitectura innovadora: El nuevo diseño modular permitirá la interconexión de múltiples procesadores cuánticos, potenciando exponencialmente su capacidad de procesamiento.

Aplicaciones transformadoras: Se espera que este ordenador cuántico de última generación abra nuevas fronteras en la resolución de problemas complejos, la simulación de sistemas cuánticos y el desarrollo de algoritmos revolucionarios.

Atendiendo a los hitos alcanzados, tenemos

Osprey: En 2022, IBM presentó Osprey, un procesador cuántico de 433 qubits, el más potente de la época.

Kookaburra: Actualmente en desarrollo, Kookaburra será un procesador multichip con 1.386 qubits, un paso importante hacia la meta final.

Estado del arte actual:

La tecnología cuántica aún se encuentra en sus primeras etapas de desarrollo, pero los avances de IBM y otros actores clave están acelerando su progreso.

Los desafíos técnicos, como la corrección de errores y la decoherencia cuántica, siguen siendo obstáculos importantes que deben superarse. Esto tiene que ver con el "ruido", que mencionamos más adelante.

El objetivo de IBM es construir un ordenador cuántico de 100.000 qubits para finales de la década, posicionándose como líder en esta nueva era de la computación.

Se espera que este hito tecnológico tenga un impacto profundo en diversos sectores, impulsando la innovación y el desarrollo en áreas como la medicina, la ciencia de materiales, la inteligencia artificial y la seguridad cibernética.

Otras conclusiones:

El desarrollo de ordenadores cuánticos a gran escala plantea interrogantes éticos y legales que deben ser abordados.

La colaboración internacional y la inversión sostenida en investigación serán cruciales para alcanzar el pleno potencial de esta tecnología disruptiva. [36]

Estado del arte actual:

Las tecnologías cuánticas están en rápido desarrollo y podrían suponer una amenaza significativa para la criptografía actual basada en algoritmos como RSA y ECDSA12.

La criptografía post-cuántica es un campo de investigación que busca desarrollar nuevos algoritmos y protocolos criptográficos resistentes a ataques cuánticos

"El Instituto Nacional de Normas y Tecnología (NIST) de Estados Unidos ha iniciado el proceso de selección, evaluación y normalización de algoritmos de post-quantum cryptography" [37].

Actualmente, no existe una solución única y definitiva para la criptografía post-cuántica. Se están investigando y desarrollando diversas propuestas, pero aún no hay un estándar claro [38].

Riesgos de la criptografía actual:

Los ataques cuánticos podrían romper la confidencialidad e integridad de las comunicaciones protegidas por la criptografía actual [39].

Esto podría tener graves consecuencias para la seguridad nacional, la privacidad individual y la economía digital. Esto está estrechamente relacionado con los cifrados usados por empresa, al poder cuestionar si en un futuro de no más de 5 o 7 años seguirán siendo seguros. La reciente ley europea RGPD habla de la protección de nuestros datos personales.

- Se estima que los ataques cuánticos podrían ser viables en la próxima década. [40]

Cifrados y usos:

- La criptografía actual se utiliza para proteger una amplia gama de datos y comunicaciones, incluyendo transacciones financieras, comunicaciones gubernamentales y militares, registros médicos, datos de identidad e infraestructuras críticas. [41]

Objetivos clave de Europa:

- El documento de la EPC establece una serie de objetivos clave para la criptografía post-cuántica en Europa: Desarrollar y adoptar estándares de criptografía post-cuántica, Invertir en investigación y desarrollo en esta área, Aumentar la sensibilización sobre los riesgos de la criptografía actual, Preparar a las organizaciones públicas y privadas para la transición a la criptografía post-cuántica, Cooperar con otros países y organizaciones internacionales. [42]

Fecha límite:

- El documento de la EPC establece una fecha límite de 2024 para que las organizaciones europeas comiencen a planificar la transición a la criptografía post-cuántica.
- Se espera que la adopción generalizada de la criptografía post-cuántica se produzca en la próxima década. [32] [43]

Comparación entre Europa y Estados Unidos:

- Tanto Europa como Estados Unidos están invirtiendo en investigación y desarrollo de la criptografía post-cuántica. Sin embargo, hay algunas diferencias clave en sus enfoques: Europa está adoptando un enfoque más colaborativo y está trabajando para

desarrollar estándares abiertos. Estados Unidos está adoptando un enfoque más competitivo y está permitiendo que el mercado desarrolle soluciones.

En otras palabras:

- La criptografía post-cuántica es un tema complejo y crucial para la seguridad nacional y la economía digital. Es importante que tanto Europa como Estados Unidos continúen invirtiendo en investigación y desarrollo en esta área y que trabajen juntos para desarrollar soluciones seguras y escalables.

Dicho documento, propone **seis recomendaciones principales** para que la **Unión Europea** (**UE**) se prepare para la **era de la computación cuántica y proteja su ciberseguridad**:

1. **Plan de acción coordinado de la UE**: Se plantea la creación de un plan con objetivos, plazos y mecanismos de control para supervisar la migración nacional hacia el cifrado post-cuántico (resistente a ataques cuánticos).

2. **Grupo de expertos en ENISA**: Se propone establecer un grupo de expertos dentro de la Agencia de Ciberseguridad de la Unión Europea (ENISA) para intercambiar buenas prácticas e identificar obstáculos en la transición.

3. **Prioridades y agilidad criptográfica**: Recomienda establecer prioridades para la transición y promover la adaptabilidad de los sistemas criptográficos para responder a vulnerabilidades emergentes.

4. **Coordinación política**: Aboga por la coordinación entre la Comisión Europea, los estados miembros, las agencias nacionales de ciberseguridad y ENISA, con el fin de definir prioridades tecnológicas e identificar casos de uso relevantes para tecnologías cuánticas seguras.

5. **Coordinación técnica**: Propone abordar las brechas de investigación en tecnologías cuánticas seguras, como el desarrollo de nodos cuánticos para conexiones de larga distancia en la distribución cuántica de claves.

6. **Uso de "sandboxes":** Se recomienda explorar el **uso de entornos aislados** (sandboxes) para **acelerar el desarrollo de aplicaciones** cercanas a la realidad de las tecnologías de la información cuántica. [32]

¿Qué es un Qúbit? ¿Qué lo diferencia de un bit de computación clásica?

En el corazón de la computación cuántica reside el **Qúbit** (abreviatura de **bit cuántico, en inglés quantum-bit**), una unidad fundamental de información que revoluciona el paradigma computacional clásico. A diferencia de los bits clásicos, que solo pueden existir en estados binarios (0 o 1), donde cada uno de los transistores microscópicos tiene o no tiene la suficiente electricidad para marcar cada uno de ellos esa unidad de información booleana, los qubits aprovechan los principios de la mecánica cuántica para existir en una superposición de ambos estados simultáneamente. Esta propiedad única, conocida como superposición cuántica, junto con el entrelazamiento cuántico, permite a las computadoras cuánticas realizar cálculos y resolver problemas que son intratables para las computadoras clásicas.

Se entiende por superposición en este sentido, la dualidad de dos estados a la vez, o, mejor dicho, un estado que es ambos, representable en la "esfera de Bloch". [52]

Para entender la naturaleza de un qubit, debemos hablar de la física cuántica. En este mundo subatómico, las partículas no se comportan como objetos clásicos predecibles, sino que exhiben propiedades probabilísticas y dualidad onda-partícula [53], como ya ocurrió con los fotones que componen la luz, que ya describió [ver referencias Einstein dualidad] . Los qubits se pueden implementar utilizando diversos sistemas físicos, como los electrones con espín, los fotones polarizados o los iones atrapados. La elección del sistema físico depende de los requisitos específicos de la aplicación y las tecnologías disponibles.

Un qubit básico se representa matemáticamente por un vector de estado $|\psi\rangle$, que es una combinación lineal de los estados base $|0\rangle$ y $|1\rangle$:

$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$

donde α y β son números complejos que satisfacen la condición de normalización $|\alpha|^2 + |\beta|^2 = 1$. La probabilidad de medir el qubit en el estado $|0\rangle$ o $|1\rangle$ está dada por $|\alpha|^2$ y $|\beta|^2$, respectivamente.

La superposición cuántica permite a un qubit representar múltiples valores simultáneamente, lo que se traduce en un aumento exponencial en la potencia computacional. Imagine una computadora clásica con 30 bits; solo puede almacenar un número de 0 a 2^30 - 1 (aproximadamente 10^9). En cambio, una computadora cuántica con 30 qubits puede representar una superposición de todos estos números simultáneamente, desbloqueando un potencial computacional sin precedentes.

El entrelazamiento cuántico, otro fenómeno fundamental en la mecánica cuántica, surge cuando dos o más qubits se conectan de manera que sus estados se vuelven interdependientes. Medir el estado de un qubit entrelazado instantáneamente determina el estado de los demás qubits entrelazados, incluso si están separados por grandes distancias. Esta correlación no local, que desafía la intuición clásica, permitiría a las computadoras cuánticas realizar tareas como la teletransportación de un estado cuántico, y la computación cuántica distribuida. Esto sucede cuando dos estados cuánticos cada uno en un átomo distinto, por decir un objeto físico, por muy separados en distancia que estén uno de otro, si realmente están ambos entrelazados, lo normal es que ambos siempre den el estado contrario al otro, es decir, que al

comprobar el estado sea “más cercano” al 0 o al 1. Esto sucede cuando queremos observar o medir un estado cuántico, porque de alguna forma ya no somos un observador pasivo que por “ver” o “medir” no influimos, sino que obligamos a determinar de cuál estado se está más cerca, aunque no sea realmente ningún estado de ambos.

La viabilidad de los sistemas de múltiples qubits es un área de investigación activa en la computación cuántica. La construcción y el mantenimiento de qubits estables y confiables, así como la minimización del ruido y la decoherencia, son desafíos técnicos importantes que deben abordarse para lograr la escalabilidad y el rendimiento práctico de las computadoras cuánticas a gran escala. [54]

Corrección de errores y decoherencia cuántica como desafíos técnicos significativos en computación cuántica

En cambio, cabe destacar que el “ruido” y los fallos en los cálculos de cómputo son un problema que aún se deben resolver:

La decoherencia, los errores en las puertas cuánticas y la necesidad de técnicas de corrección de errores son fuentes de fricción que dificultan el progreso de la computación cuántica. [44]

En un reportaje de MIT Technology Review, se destaca que el progreso en la computación cuántica en 2023 se caracterizará por la culminación del arduo trabajo para conseguir que los chips se comuniquen entre sí y solventar el problema del ruido. [45]

Los dos mayores retos que es necesario superar para hacer posible la puesta a punto de los ordenadores cuánticos plenamente funcionales son la implementación de un sistema de corrección de errores que garantice que los resultados que leemos son los correctos, y también el escalado del número de cúbits que pueden computar en conjunto sin dar fallos, de forma estable. [46]

Los investigadores que trabajan en el campo de la computación cuántica están intentando poner a punto qubits de más calidad; desarrollar sistemas de corrección de errores y encontrar nuevos algoritmos. [46]

Un artículo en el blog Think Big menciona que “para lograr una computación cuántica estable, es necesario desarrollar técnicas de corrección de errores que permitan identificar y corregir estos errores de manera efectiva”. [47]

Corrección de errores de cómputo en los qubits; expectativas para los próximos 9 años

IBM vs. Quera e Intel

Por parte de IBM, la corrección de errores será posible a partir de 2033:

- **Hoja de ruta:** IBM ha establecido una ambiciosa hoja de ruta para la corrección de errores, con el objetivo de lograr un **computador cuántico a gran escala con corrección de errores para el año 2033**.
- **Estrategia:** IBM se enfoca en desarrollar **códigos de corrección de errores escalables y eficientes**, utilizando técnicas como el **código Reed-Solomon** y **códigos de concatenación**.
- **Impacto:** La corrección de errores de IBM permitirá realizar cálculos cuánticos complejos con mayor precisión y confiabilidad, impulsando avances en áreas como la **inteligencia artificial**, la **química computacional**, la **medicina de precisión** y la **criptografía cuántica**.

Por el lado contrario, con la alianza entre la “startup” o empresa emergente Quera con Intel, se espera que sea antes, de aquí a 2 años en 2026:

- **Alianza:** Quera, una empresa de computación cuántica, se ha asociado con Intel para desarrollar un **computador cuántico con corrección de errores para el año 2026**.
- **Estrategia:** Quera e Intel se enfocan en un enfoque de **computación cuántica distribuida**, utilizando **muchos qubits pequeños y menos propensos a errores** conectados a través de una red.
- **Impacto:** La corrección de errores de Quera e Intel podría permitir la construcción de **computadores cuánticos más compactos y económicos**, acelerando la adopción de la tecnología cuántica en diversos sectores. [48]

Una tabla comparativa de plazos e impacto de ambos caminos de corrección de errores:

Característica	IBM	Quera e Intel
Año objetivo	2033	2026
Estrategia	Códigos de corrección de errores escalables	Computación cuántica distribuida
Impacto	Cálculos cuánticos complejos con mayor precisión y confiabilidad	Computadores cuánticos más compactos y económicos

Computación cuántica con iones fríos atrapados a partir del artículo "A Quantum Computer with Trapped Ions"

La computadora cuántica se basa en iones individuales atrapados en un campo eléctrico y enfriados a temperaturas cercanas al cero absoluto. Cada ión funciona como un qubit, la unidad fundamental de información cuántica. Las operaciones cuánticas se realizan utilizando láseres para manipular los estados cuánticos de los iones. Entre sus posibilidades, la computación cuántica con iones atrapados aprovecha las propiedades únicas de la mecánica cuántica para realizar cálculos que son imposibles para las computadoras clásicas. Los iones atrapados proporcionan un sistema aislado y bien controlado, ideal para la implementación de algoritmos cuánticos.

Para que puedan funcionar, los iones deben estar atrapados con precisión y enfriados a temperaturas extremadamente bajas para minimizar la decoherencia cuántica, que puede corromper los estados cuánticos. La manipulación láser debe ser precisa y controlada para realizar las operaciones cuánticas deseadas.

Capacidad de cálculo: El número de qubits que se pueden utilizar en una computadora cuántica con iones atrapados está limitado por la tecnología actual de atrapamiento y enfriamiento.

Sin embargo, se han demostrado pequeñas computadoras cuánticas con unos pocos qubits y se están desarrollando sistemas con mayor número de qubits.

Otras ideas principales:

El artículo describe un esquema para la implementación de un qubit lógico utilizando dos estados de iones atrapados.

Se presentan ejemplos de cómo se pueden realizar operaciones cuánticas básicas, como la puerta CNOT, utilizando láseres.

Se discuten los desafíos técnicos que deben superarse para construir una computadora cuántica escalable con iones atrapados.

En resumen:

El artículo "A Quantum Computer with Trapped Ions" presenta una visión general de la computación cuántica con iones atrapados, destacando su potencial para realizar cálculos que son imposibles para las computadoras clásicas. Si bien existen desafíos técnicos que deben superarse, la computación cuántica con iones atrapados es un área de investigación prometedora con el potencial de revolucionar la informática en el futuro. [49]

Políticas de la Unión Europea en materia de computación cuántica

Objetivo: Posicionar a Europa como líder global en la computación cuántica, aprovechando su potencial para transformar sectores clave como la salud, la energía, la seguridad y el transporte.

Ejes principales:

- Inversión: Aumentar la inversión pública y privada en investigación y desarrollo de tecnologías cuánticas.
- Colaboración: Fomentar la colaboración entre academia, industria y sector público a nivel europeo e internacional.
- Desarrollo de talento: Capacitar a profesionales en las habilidades necesarias para la computación cuántica.
- Marco regulatorio: Establecer un marco regulatorio adecuado para la innovación y el uso responsable de las tecnologías cuánticas.
- Infraestructura: Desarrollar una infraestructura segura y escalable para la computación cuántica.

Aplicaciones:

- Medicina: Descubrimiento de nuevos fármacos y terapias, diagnóstico personalizado y desarrollo de medicina preventiva.
- Materiales: Diseño de nuevos materiales con propiedades avanzadas, como mayor resistencia o conductividad.
- Energía: Optimización de redes eléctricas, desarrollo de nuevas fuentes de energía y almacenamiento de energía.
- Seguridad: Criptografía resistente a ataques cuánticos, protección de datos y ciberseguridad.
- Transporte: Optimización de rutas de transporte, desarrollo de vehículos autónomos y gestión del tráfico.

Impacto:

La computación cuántica tiene el potencial de generar un impacto económico y social significativo, creando nuevos empleos, impulsando la competitividad de las empresas europeas y mejorando la calidad de vida de los ciudadanos.

Desafíos:

- Complejidad tecnológica: La computación cuántica es una tecnología compleja y todavía en desarrollo.
- Alto costo: La construcción y operación de computadores cuánticos es costosa.
- Falta de talento: Existe una escasez de profesionales cualificados en el campo de la computación cuántica.
- Amenazas a la seguridad: La computación cuántica puede suponer una amenaza para la seguridad de las comunicaciones y los datos.

Conclusión:

La Estrategia Digital de la UE para la Computación Cuántica establece una hoja de ruta ambiciosa para posicionar a Europa como líder en esta tecnología disruptiva. El éxito de la estrategia dependerá de la colaboración efectiva entre todos los actores relevantes y de la capacidad de abordar los desafíos existentes. [50]

Ignacio Cirac y sus contribuciones a la computación cuántica

¿Quién es Ignacio Cirac?

Ignacio Cirac es un físico teórico español reconocido a nivel mundial por sus contribuciones pioneras en el campo de la computación cuántica. Actualmente dirige el Instituto Max Planck de Óptica Cuántica en Garching, Alemania.

Sus contribuciones a la viabilidad de la computación cuántica:

Algoritmos cuánticos: Cirac ha desarrollado algoritmos cuánticos eficientes para resolver problemas complejos en áreas como la química cuántica, la simulación de sistemas cuánticos y la optimización.

Arquitecturas de computadores cuánticos: Ha propuesto arquitecturas innovadoras para computadores cuánticos, incluyendo el uso de iones atrapados y circuitos superconductores.

Corrección de errores cuánticos: Ha desarrollado técnicas para corregir errores en los sistemas cuánticos, un desafío crucial para la construcción de computadores cuánticos prácticos.

Eficacia de la computación cuántica:

Las investigaciones de Cirac han demostrado el potencial de la computación cuántica para resolver problemas que son **intratables** para las computadoras clásicas, como la **factorización de números grandes** o la **simulación de sistemas moleculares complejos**.

Aplicaciones de la computación cuántica:

Las aplicaciones potenciales de la computación cuántica incluyen:

Desarrollo de nuevos medicamentos y materiales: La simulación de sistemas cuánticos a nivel molecular podría acelerar el descubrimiento de nuevos fármacos y materiales.

Optimización financiera: La computación cuántica podría utilizarse para optimizar carteras de inversión y resolver problemas de logística complejos. Por ejemplo, usando la optimización lineal.

Inteligencia artificial: La computación cuántica podría mejorar el rendimiento de los algoritmos de aprendizaje automático y permitir el desarrollo de nuevas aplicaciones de IA.

Ideas principales sobre las contribuciones de Ignacio Cirac:

Desarrollo de algoritmos cuánticos eficientes.

Propuesta de arquitecturas innovadoras para computadores cuánticos.

Investigación en técnicas de corrección de errores cuánticos.

Demostración del potencial de la computación cuántica para resolver problemas complejos.

Criptografía post-cuántica:

Las investigaciones de Cirac en computación cuántica también han tenido un impacto significativo en el desarrollo de la **criptografía post-cuántica**. La criptografía actual se basa en algoritmos que son vulnerables a los ataques de las computadoras cuánticas. Cirac y otros investigadores están trabajando en el desarrollo de nuevos algoritmos criptográficos que sean resistentes a estos ataques.

En resumen:

Ignacio Cirac es un científico pionero que ha hecho contribuciones fundamentales al campo de la computación cuántica. Sus investigaciones han ayudado a demostrar la viabilidad de la computación cuántica y han abierto el camino para el desarrollo de nuevas aplicaciones en diversas áreas, incluyendo la criptografía post-cuántica, a pesar de que al inicio de su trayectoria fuese en la óptica y la luz usando sus estudios en física. [51]

Probando código Python y la librería Qiskit para su posterior ejecución en IBM-Q

Hoy día, si le preguntamos a una inteligencia artificial en forma de LLM [55](Large Language Model) como, por ejemplo, Gémini [56], que está disponible online en internet, algo así para hacer un código base, algo de lo que poder ir probando y haciendo modificaciones, nos dará un resultado así.

Consulta: "haz un código en Python para factorizar uno por uno todos los números de una lista aleatoria de 5 números,

usando el algoritmo de Shor y la librería Qiskit. Este código se usará en IBM quantum platform, con ordenadores

cuánticos, y debe estar optimizado para ello, y tener en cuenta que se usará un ordenador con 127 qubits.

Una vez hecho el código, debes comentar cada línea el código explicando lo que hace, crea, almacena, procesa, lo que sea."

Este sería el resultado, en distintas ocasiones que se le pregunta:

```
import qiskit
from qiskit import QuantumCircuit, QuantumRegister, ClassicalRegister
import random

def factorize_number(number):
    """
    Factorizes a given integer 'number' using Shor's algorithm on a simulated quantum computer.

    Args:
        number (int): The integer to be factorized.

    Returns:
        List[int]: A list of factors of the given number, or an empty list if no factors are found.
    """
```

```
# Check if the number is even
if number % 2 == 0:
    return [2]

# Convert the number to binary representation
binary_string = bin(number)[2:]
num_qubits = len(binary_string)

# Ensure that the number of qubits is less than or equal to the available qubits
if num_qubits > 127:
    raise ValueError("Number of qubits exceeds the available qubits (127)")

# Initialize quantum registers
qreg_n = QuantumRegister(num_qubits)  # Number register
qreg_a = QuantumRegister(num_qubits)  # Oracle register
creg = ClassicalRegister(num_qubits)  # Classical register

# Create the quantum circuit
circuit = QuantumCircuit(qreg_n, qreg_a, creg)

# Prepare the initial state
circuit.x(qreg_n)  # Apply Hadamard gates to all qubits in the number register

# Implement the quantum Fourier transform (QFT) on the number register
for i in range(num_qubits):
    for j in range(i + 1):
        circuit.cx(qreg_n[i], qreg_n[j])
        circuit.h(qreg_n[j])
```

```
# Implement the oracle operation
for i in range(num_qubits):
    if binary_string[i] == "1":
        circuit.cx(qreg_a[i], qreg_n[i])

# Implement the inverse quantum Fourier transform (QFT) on the number register
for i in range(num_qubits - 1, -1, -1):
    for j in range(i):
        circuit.cx(qreg_n[i], qreg_n[j])
        circuit.h(qreg_n[j])

# Measure the qubits
for i in range(num_qubits):
    circuit.measure(qreg_n[i], creg[i])

# Simulate the circuit
backend = BasicAer.get_backend()  # Use a simulator for this example
job = backend.run(circuit)
result = job.result().get_counts()

# Analyze the results
factors = []
for binary_result, count in result.items():
    if count > 0:
        # Convert the binary result to decimal
        decimal_result = int(binary_result, 2)

        # Check if the decimal result is a factor of the original number
        if number % decimal_result == 0 and decimal_result != 1 and decimal_result != number:
            factors.append(decimal_result)
```

```
    return factors

def main():
    """
    Generates a random list of 5 integers and factorizes each number using Shor's algorithm.
    """

    # Generate a random list of 5 integers between 2 and 100
    numbers = [random.randint(2, 100) for _ in range(5)]

    # Factorize each number in the list
    for number in numbers:
        factors = factorize_number(number)
        print(f"Factors of {number}: {factors}")

if __name__ == "__main__":
    main()
```

Ahora, otro intento, opción 2 de possible Código en Python usando Qiskit:

```
import qiskit
from qiskit import QuantumCircuit, QuantumRegister, ClassicalRegister
import random

def factorize_number(number):
    # Convert the number to binary representation
    binary_string = bin(number)[2:]
    num_qubits = len(binary_string)
```

```
    # Check if the number is even or odd
    if number % 2 == 0:
        # If the number is even, 2 is a factor
        print("Factor found:", 2)
        return 2

    # Initialize quantum registers
    qreg_n = QuantumRegister(num_qubits)  # Number register (n qubits)
    qreg_a = QuantumRegister(num_qubits)  # Oracle register (n qubits)
    creg = ClassicalRegister(num_qubits)  # Classical bits (n bits)

    # Create the quantum circuit
    circuit = QuantumCircuit(qreg_n, qreg_a, creg)

    # Prepare the initial state
    circuit.h(qreg_n)  # Apply Hadamard gates to all qubits in the number register

    # Implement the quantum Fourier transform (QFT) on the number register
    for i in range(num_qubits):
        for j in range(i + 1):
            circuit.cx(qreg_n[i], qreg_n[j])
            circuit.h(qreg_n[j])

    # Implement the oracle operation
    for i in range(num_qubits):
        if binary_string[i] == "1":
            circuit.cx(qreg_a[i], qreg_n[i])

    # Implement the inverse quantum Fourier transform (QFT) on the number register
```

```
    for i in range(num_qubits - 1, -1, -1):
        for j in range(i):
            circuit.cx(qreg_n[i], qreg_n[j])
            circuit.h(qreg_n[j])

    # Measure the qubits
    for i in range(num_qubits):
        circuit.measure(qreg_n[i], creg[i])

    # Simulate the circuit
    backend = BasicAer.get_backend()
    job = backend.run(circuit)
    result = job.result().get_counts()

    # Analyze the results
    for binary_result, count in result.items():
        if count > 0:
            # Convert the binary result to decimal
            decimal_result = int(binary_result, 2)

            # Check if the decimal result is a factor of the original number
            if number % decimal_result == 0 and decimal_result != 1 and decimal_result != number:
                print("Factor found:", decimal_result)
                return decimal_result

    # No factors found
    print("No factors found for", number)
    return None

def main():
```

```
    # Generate a random list of 5 numbers
    numbers = [random.randint(3, 100) for _ in range(5)]

    # Factorize each number in the list
    for number in numbers:
        factorize_number(number)

if __name__ == "__main__":
    main()
```

Opción 3:

```
import Qiskit
from qiskit import QuantumCircuit, QuantumRegister, ClassicalRegister
import random
def factorize_number(number):
```

```
# Convert the number to binary representation
binary_string = bin(number)[2:]
num_qubits = len(binary_string)

# Check if the number is even or odd
if number % 2 == 0:
    # If the number is even, 2 is a factor
    print("Factor found:", 2)
    return 2

# Initialize quantum registers
qreg_n = QuantumRegister(num_qubits)  # Number register (n qubits)
qreg_a = QuantumRegister(num_qubits)  # Oracle register (n qubits)
creg = ClassicalRegister(num_qubits)  # Classical bits (n bits)

# Create the quantum circuit
circuit = QuantumCircuit(qreg_n, qreg_a, creg)
```

```
# Prepare the initial state
circuit.h(qreg_n)  # Apply Hadamard gates to all qubits in the number register

# Implement the quantum Fourier transform (QFT) on the number register
for i in range(num_qubits):
    for j in range(i + 1):
        circuit.cx(qreg_n[i], qreg_n[j])
        circuit.h(qreg_n[j])

# Implement the oracle operation
for i in range(num_qubits):
    if binary_string[i] == "1":
        circuit.cx(qreg_a[i], qreg_n[i])

# Implement the inverse quantum Fourier transform (QFT) on the number register
for i in range(num_qubits - 1, -1, -1):
    for j in range(i):
        circuit.cx(qreg_n[i], qreg_n[j])
```

```
        circuit.h(qreg_n[j])


# Measure the qubits
for i in range(num_qubits):
    circuit.measure(qreg_n[i], creg[i])


# Simulate the circuit
backend = BasicAer.get_backend()
job = backend.run(circuit)
result = job.result().get_counts()


# Analyze the results
for binary_result, count in result.items():
    if count > 0:
        # Convert the binary result to decimal
        decimal_result = int(binary_result, 2)


        # Check if the decimal result is a factor of the original number
```

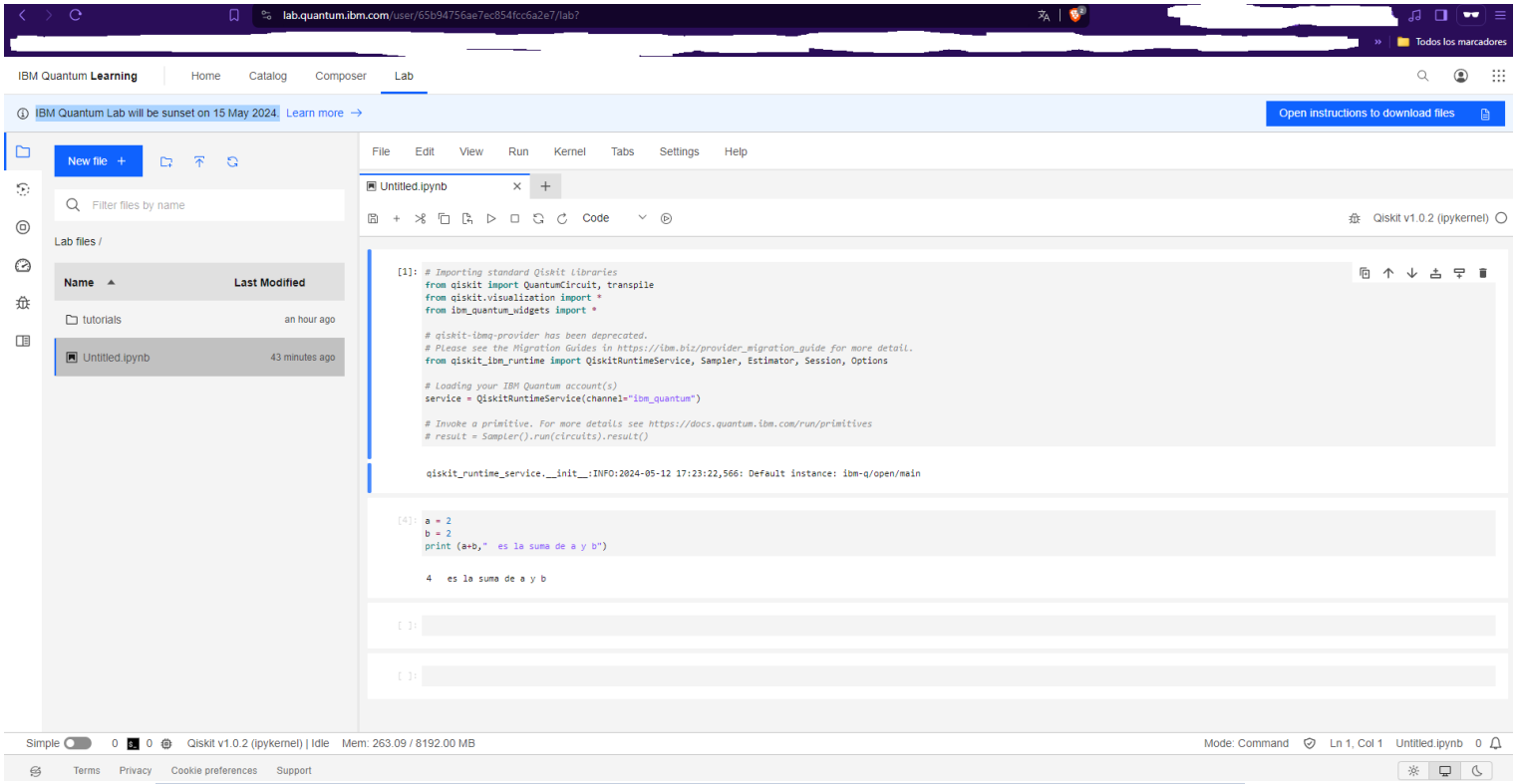
```
            if number % decimal_result == 0 and decimal_result != 1 and decimal_result != number:
                print("Factor found:", decimal_result)
                return decimal_result

    # No factors found
    print("No factors found for", number)
    return None

def main():
    # Generate a random list of 5 numbers
    numbers = [random.randint(3, 100) for _ in range(5)]

    # Factorize each number in the list
    for number in numbers:
        factorize_number(number)

if __name__ == "__main__":
    main()
```



lab.quantum.ibm.com/user/65b94756ae7ec854fcc6a2e7/lab?

File Edit View Run Kernel Tabs Settings Help

Untitled.ipynb

Code

```
[1]: # Importing standard Qiskit libraries
from qiskit import QuantumCircuit, transpile
from qiskit.visualization import *
from ibm_quantum_widgets import *

# qiskit-ibmq-provider has been deprecated.
# Please see the Migration Guides in https://ibm.biz/provider_migration_guide for more detail.
from qiskit_ibm_runtime import QiskitRuntimeService, Sampler, Estimator, Session, Options

# Loading your IBM Quantum account(s)
service = QiskitRuntimeService(channel="ibm_quantum")

# Invoke a primitive. For more details see https://docs.quantum.ibm.com/run/primitives
# result = Sampler().run(circuits).result()
```

```
qiskit_runtime_service.__init__:INFO:2024-05-12 17:23:22,566: Default instance: ibm-q/open/main
```

```
[4]: a = 2
b = 2
print (a+b,"  es la suma de a y b")
```

```
4   es la suma de a y b
```

La posterior ejecución de pruebas de código en ordenadores de IBM se incluye en la presentación de PowerPoint, que se mostrará el día de la defensa de este **Trabajo de Fin de Grado.**

El futuro de la criptografía post-cuántica: Los cifrados finalistas del concurso del NIST: la criptografía resistente a la computación cuántica

El artículo ¿Está preparado para la era de la computación cuántica? aborda la importancia de la criptografía cuántica segura y la necesidad de que las empresas comiencen a desarrollar una estrategia cuántica segura ahora.

El NIST se encuentra actualmente en el proceso de desarrollar algoritmos cuánticos seguros, e IBM ha participado en la creación de tres de los cuatro finalistas, que son. La era cuántica está llegando y las empresas necesitan estar preparadas.

Puntos clave del artículo:

La computación cuántica representa una amenaza significativa para la criptografía actual.

Los algoritmos cuánticos pueden romper fácilmente la criptografía asimétrica, como RSA y ECC, que se utilizan ampliamente en la actualidad.

La criptografía cuántica segura es una nueva forma de criptografía que es resistente a los ataques de las computadoras cuánticas.

El NIST está desarrollando estándares para la criptografía cuántica segura, y se espera que los primeros estándares se publiquen en 2024.

Las empresas deben comenzar a desarrollar una estrategia cuántica segura ahora para estar preparadas para la era cuántica.

El artículo también proporciona algunas recomendaciones para que las empresas comiencen a desarrollar una estrategia cuántica segura:

Realizar una evaluación de riesgos: Las empresas deben evaluar su riesgo de exposición a ataques cuánticos.

Identificar activos críticos: Las empresas deben identificar sus activos críticos que necesitan protección cuántica.

Comenzar a investigar y probar soluciones de criptografía cuántica segura.

Desarrollar un plan de implementación: Las empresas deben desarrollar un plan para implementar soluciones de criptografía cuántica segura.

Educar y capacitar a los empleados: Las empresas deben educar y capacitar a sus empleados sobre la criptografía cuántica segura.

La era cuántica está llegando, y las empresas necesitan estar preparadas. La criptografía cuántica segura es una herramienta esencial para proteger los datos y las comunicaciones en la era cuántica. Las empresas que comiencen a desarrollar una estrategia cuántica segura ahora estarán mejor posicionadas para el éxito en el futuro. [57]

El Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST) organizó un concurso para seleccionar algoritmos de criptografía post-cuántica adecuados para su promoción como estándares1. Los algoritmos propuestos por equipos de investigación internacionales fueron estudiados por expertos independientes en busca de posibles vulnerabilidades y debilidades1.

Los algoritmos finalistas del concurso son los siguientes:

CRYSTALS-Kyber: Este algoritmo fue el ganador entre los algoritmos universales que se pueden utilizar para proteger la transmisión de información en redes informáticas. Sus puntos fuertes son un tamaño de clave relativamente pequeño y una alta velocidad1.

CRYSTALS-Dilithium: Este algoritmo es altamente eficiente y se recomienda como algoritmo principal para firmas digitales1.

FALCON: Este algoritmo también es altamente eficiente y se centra en soluciones que requieren un tamaño de firma mínimo1.

SPHINCS+: Aunque este algoritmo va a la zaga de los dos primeros algoritmos en términos de tamaño de firma y velocidad, se quedó como una alternativa entre los finalistas, ya que se basa en principios matemáticos completamente diferentes1.

Además de estos, se han identificado otros cuatro algoritmos de uso general: **BIKE**, **Classic McEliece**, **HQC** y **SIKE**, que deben mejorarse1. Los autores de estos algoritmos tienen la oportunidad de actualizar las especificaciones y eliminar las deficiencias en las implementaciones hasta el 1 de octubre, después de lo cual también pueden ser incluidos entre los finalistas. [58]

Criptografía post-cuántica: riesgos y oportunidades

Citando una investigación sobre la computación cuántica, este es parte del capítulo de la criptografía post-cuántica, traducido al español:

"Convencionalmente, la seguridad de las primitivas criptográficas clásicas (por ejemplo, RSA, Diffie-Hellman, etc.) depende de los difíciles problemas de la aritmética discreta, la factorización de números primos enteros y los logaritmos discretos de curva elíptica. Lamentablemente, estas primitivas criptográficas actuales basadas en problemas tan difíciles podrían resolverse teóricamente en un breve espacio de tiempo utilizando las posibles aplicaciones de los ordenadores cuánticos. Los inminentes ataques que los algoritmos cuánticos plantean a los protocolos criptográficos convencionales han promovido un sentimiento de urgencia en el diseño de esquemas alternativos para mitigar los ataques cuánticos. Tales alternativas se caracterizan generalmente como criptografía post-cuántica (PQC). Estos esquemas pueden hacer frente con eficacia a los retos que plantean los adversarios cuánticos. Esto lleva a muchos a preguntarse por la criptografía post-cuántica [64 – 1]. Los protocolos utilizados en la criptografía post-cuántica pueden agruparse generalmente en cinco tipos: basados en códigos, basados en hash, basados en celosías, multifacéticos y esquemas de isogénica elíptica de curvas "supersingulares". [64 – 2]

Al poner en peligro la seguridad de los datos de defensa cifrados, las mayores capacidades de procesamiento de la computación cuántica dejan al descubierto las posibles deficiencias de las actuales técnicas de cifrado. El enfoque "recoger ahora, descifrar después" es auténtico, ya que permite a los atacantes almacenar material cifrado hasta que la tecnología de descifrado esté más avanzada [64 – 3]. Dado que la gravedad de sus fallos determina hasta qué punto está

dispuesta a asumir riesgos, la industria militar no puede permitirse ignorar o minimizar el riesgo.” [64]

Otras perspectivas de la cuántica de la mano de expertos

En una charla con Eduardo Sáenz de Cabezón, matemático, sobre la computación cuántica, su funcionamiento y su capacidad de romper cifrados, podemos deducir varias cosas: no tendremos un ordenador disponible para poder usarlo en el ámbito doméstico, en casa, en un plazo estimado de al menos 30 años, aproximadamente [59]. En cualquier caso, no podremos tenerlos físicamente la población común en casa en el corto plazo. En la seguridad de los cifrados de la criptografía, de la que confiamos todos los días para transacciones bancarias, los certificados que validan la propiedad de nuestra vivienda, entre otros usos, también sabemos que de momento no se pueden romper. Por su limitación tanto de cantidad de información que pueden manejar estos ordenadores al mismo tiempo, como del tiempo máximo de ejecución que pueden tener estos qubits mientras conservan ese “tiempo de coherencia cuántica”, sin que pierdan información y se puedan seguir leyendo su estado, 0 o 1 de forma no errónea. [60]

En una entrevista con José Ignacio Gentile, informático y “streamer” en redes sociales, vemos resumido sobre el funcionamiento de los ordenadores cuánticos, sus aplicaciones y perspectivas de futuro [61]

Los ordenadores cuánticos usan qubits que, para funcionar sin tener interferencias entre ellos, sin que las partículas interaccionen entre ellas, tienen que estar a una temperatura de milésimas de grado Celsius por encima del 0 absoluto, a mili-kelvins. [62]

En palabras de una ingeniera de IBM Quantum: los 2 principales problemas son la “coherencia cuántica”, es decir, el tiempo durante el cual un qubit conserva su estado cuántico no siendo ni 0 ni 1, y pudiendo ser leído sin errores. El otro, la escalabilidad del número de qubits que pueden operar simultáneamente juntos sin fallar.

Terminología en computación cuántica

Estos términos han sido parafraseados de la fuente

➔ QUBIT

En el ámbito de la computación clásica, un bit de memoria representa información como 0 o 1, pero no ambos simultáneamente. Si el bit al forzar su lectura con un lector del circuito DC 1, la probabilidad del estado de carga del transistor es 1, y si el estado está en modo de descarga, la probabilidad de 0 es 1. Las computadoras cuánticas almacenan información en forma de cúbits. El qubit es la unidad básica de información en la computación cuántica, capaz de representar simultáneamente 0, 1, o ambos.

En la computación clásica, el estado de un transistor representa el bit, mientras que, en la computación cuántica, el estado físico de una partícula cuántica representa el qubit. Este estado físico puede ser "spin arriba" o "spin abajo" en átomos, o "Polarización Horizontal" y "Polarización Vertical" en fotones. También se pueden usar dos niveles de energía, como "estado excitado" y "estado base" para las partículas cuánticas. Para representar información, el estado excitado puede representarse como 1 y el estado base como 0. Para representar el qubit, se utiliza la notación de Dirac |0≥0 |1≥1 .

➔ SUPERPOSICIÓN

- Partículas cuánticas
  - Estado excitado (1)
  - Estado fundamental (0)
  - Tercer estado
    - Simultáneamente 1 y 0

• Superposición

- a y b, como números complejos
  - Espacio vectorial bidimensional
  - Longitud 1

En ese caso, el estado de superposición de la partícula puede expresarse como

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

donde a y b son números complejos tales que $|a|^2+|b|^2=1$. Aquí, a representa la amplitud probabilística del estado base |0⟩|0\rangle|0⟩ y b representa la amplitud probabilística del estado base |1⟩|1\rangle|1⟩. Debido a la propiedad de superposición, un qubit puede incorporar múltiples valores correspondientes a varios bits en la computación clásica. Un solo qubit con 2n2^n2n estados válidos contiene 2n2^n2n valores, que pueden ser representados por n bits en la computación clásica. En otras palabras, la suma de los cuadrados de los coeficientes, en forma de números complejos, que indican la probabilidad mayor o menor de que un qubit tenga un estado 0 o 1, será siempre 1, y nunca serán todos 0. En la anterior captura donde en notación científica, se habla de coeficientes "a" para la probabilidad de que el qubit esté en un estado 0, y "b" para que sea 1, se están indicando coeficientes que en realidad son números complejos [referencia 65] . Los números complejos, pueden resumirse como una combinación de la suma de un número real con uno irreal. [referencia 66] Por ejemplo, la raíz cuadrada de menos 2 (-2).

➔ Principio de Heisenberg:

En los electrones que se mueven en torno al núcleo del átomo de la materia, hay dos variables que son excluyentes mutuamente si quieres saber a la vez su valor: posición y velocidad.

Conclusiones

La computación cuántica no amenazará a la criptografía más usada en nuestro día a día por problemas como el entrelazamiento cuántico entre partículas, y el tiempo de decoherencia entre ellas, pues el tiempo que duran dichos qubits sin quedarse en un estado fijo, para que conserven las propiedades necesarias de varios estados superpuestos de la materia, es muy bajo como para correo programas largos de ejecución como lo son los ataques de fuerza bruta contra un cifrado. En dichos ataques se prueban todas las combinaciones posibles de clave de descifrado para un algoritmo criptográfico.

Gracias al reciente éxito de la colaboración entre la fabricante de chips y CPUS Intel con QuTech [36], el instituto de investigación para la computación y el internet cuánticos de Países Bajos, (también conocido como Holanda). [68]

Podemos afirmar sin lugar a duda, que una vez los ordenadores cuánticos consigan alcanzar las promesas de empresas como IBM o Google, todos los modelos de criptografía que usamos hoy en día estarán comprometidos y obsoletos [69], como pueden serlo la multiplicación y

factorización de números en los pagos con tarjeta bancaria, o los certificados digitales que autentifican y validan la propiedad de un inmueble como lo es una casa o un hotel [59].

Bibliografía:

Imagen en portada: https://es.newsroom.ibm.com/announcements?item=122770

[1] → [31] Timeline sobre la computación cuántica: https://www.timetoast.com/timelines/historia-de-la-computacion-cuantica

"Timeline" en inglés es línea temporal. Una cronología con hechos ordenados en el tiempo.

[1] https://conceptosdelahistoria.com/innovaciones-tecnologicas/revolucion-de-la-informacion/la-computacion-cuantica/

➔ [2] https://academia-lab.com/enciclopedia/cronologia-de-la-computacion-cuantica-y-la-comunicacion/ → " (publicado en ACM SIGACT News 15(1):78–88)" →https://link.springer.com/chapter/10.1007/978-3-662-46447-2_9→ https://dl.acm.org/doi/10.1145/1008908.1008920

https://dl.acm.org/doi/pdf/10.1145/1008908.1008920 los enlaces llevaron al "paper" original de Stephen Wiesner, de la Universidad de Columbia, en Nueva York. Departamento de Física.

[2] https://academia-lab.com/enciclopedia/teorema-de-no-clonacion/

[3] https://www.phy.anl.gov/theory/staff/pbenioff/pab.html

https://www.yourtechstory.com/2020/01/10/benioff-paul-quantum-computing-theory/

https://www.quantumblogger.co/post/quantum-computing-timeline-the-80s

[4] "Models of Quantum Turing machines" es un "paper" de Paul Benioff donde discute y revisa las máquinas de Turing cuánticas. https://arxiv.org/abs/quant-ph/9708054

https://avasthiabhyudaya.medium.com/the-age-of-quantum-computing-3b4cd2ed4b43

[5] https://medium.com/@olgaokrut/who-was-yuri-manin-b5d353690387

[6] https://thequantuminsider.com/2019/12/23/quantum-godfathers-4-yuri-manin-the-accidental-quantum-icon/

https://www.nature.com/articles/s42254-021-00410-6.pdf

[7] https://ieeexplore.ieee.org/document/8203750/

[8] https://arxiv.org/abs/2106.10522

https://sgp.fas.org/othergov/doe/lanl/pubs/00783347.pdf

https://link.springer.com/chapter/10.1007/978-3-030-83274-2_2

https://www.nas.nasa.gov/pubs/ams/2020/01-23-20.html

[9] https://demonstrations.wolfram.com/DeutschsAlgorithmOnAQuantumComputer/

[10] https://www.ted.com/speakers/david_deutsch

https://www.theguardian.com/science/2022/sep/22/quantum-computing-research-physics-breakthrough

https://www.daviddeutsch.org.uk/wp-content/deutsch85.pdf

[11] https://link.springer.com/chapter/10.1007/978-3-030-23922-0_2

[12] https://scholar.google.com/citations?user=Rh7_srgAAAAJ&hl=es

[13] https://aws.amazon.com/es/blogs/quantum-computing/simons-algorithm/

[14] https://phys.org/news/2014-11-simon-algorithm-quantum-timefaster-standard.html

https://arxiv.org/abs/quant-ph/0603251

https://arxiv.org/abs/2204.11388

[15] https://physics.aps.org/articles/v15/148

[16] https://physics.aps.org/articles/v11/7

[17] https://www.nature.com/articles/nature23655

[18] https://scholar.google.com/citations?user=mkjGmJEAAAAJ

https://royalsociety.org/people/charles-bennett-35816/

https://www.societyforscience.org/alumni/notable/charles-h-bennett/

https://www.aps.org/programs/honors/prizes/landauer-bennet.cfm

[19] https://arxiv.org/abs/quant-ph/9701001

[20] https://news.mit.edu/2023/weird-weird-quantum-world-peter-shor-killian-lecture-0310

[21] https://www.quantamagazine.org/thirty-years-later-a-speed-boost-for-quantum-factoring-20231017/

[22] https://ep-news.web.cern.ch/content/interview-peter-shor

[23] https://www.classiq.io/insights/the-deutsch-jozsa-algorithm-explained

https://dl.acm.org/doi/pdf/10.1145/237814.237866

[24] https://repositorio.escuelaing.edu.co/bitstream/handle/001/774/Vega%20Fern%E1ndez,%20Cesar%20Augusto%20-%202017.pdf?sequence=2

[25] https://arxiv.org/abs/quant-ph/9701001

[26] https://docta.ucm.es/rest/api/core/bitstreams/d092e065-846a-420c-bc0b-dd9d8e3999cd/content

https://www.britannica.com/technology/quantum-computer

[27] https://news.microsoft.com/es-xl/features/en-un-logro-historico-azure-quantum-demuestra-la-fisica-antes-esquiva-necesaria-para-construir-qubits-topologicos-escalables/

[28] https://digital.csic.es/handle/10261/149405

[29] https://spectrum.ieee.org/ibm-quantum-computer-osprey

https://arxiv.org/abs/2309.15642

https://www.nature.com/articles/d41586-023-03854-1

https://www.profesionalreview.com/2020/09/17/ibm-procesadores-cuanticos-1121-qubit/

https://www.elespanol.com/omicrono/tecnologia/20221110/nuevo-cuantico-ibm-presenta-osprey-procesador-potente/717428554_0.html

https://elporvenir.mx/monitor/ibm-presenta-el-procesador-cuantico-osprey-de-433-qubits/487142

https://www.wikiversus.com/tech/ibm-anuncia-procesador-cuantico-osprey/

[30] https://arxiv.org/abs/2403.16718

https://www.ibm.com/quantum/summit-2023

https://arxiv.org/search/?query=HERON+IBM+133+qubits&searchtype=all&source=header

https://newsroom.ibm.com/2023-12-04-IBM-Debuts-Next-Generation-Quantum-Processor-IBM-Quantum-System-Two,-Extends-Roadmap-to-Advance-Era-of-Quantum-Utility

[31] https://www.nature.com/articles/s42254-021-00410-6.pdf

https://www.nature.com/articles/s42254-021-00410-6

[32] https://www.epc.eu/content/PDF/2023/Cybersecurity_DP.pdf

[33] https://csrc.nist.gov/projects/post-quantum-cryptography

[34] https://en.wikipedia.org/wiki/Quantum_cryptography

[35] https://www.epc.eu/content/PDF/2023/Cybersecurity_DP.pdf

https://www.muylinux.com/2024/02/13/the-linux-foundation-criptografia-poscuantica/

[36] https://www.technologyreview.es/s/15413/el-proximo-salto-cuantico-de-ibm-un-ordenador-de-100000-cubits

https://www.xataka.com/componentes/hito-fundamental-computacion-cuantica-intel-ha-fabricado-primer-cubit-manera-industrial

https://www.ibm.com/quantum/blog/quantum-roadmap-2033

[37] https://utimaco.com/es/servicio/base-de-conocimientos/criptografia-postcuantica/que-es-la-criptografia-postcuantica-pqc

https://csrc.nist.gov/Projects/post-quantum-cryptography/

https://keepcoding.io/blog/que-es-la-criptografia-cuantica/

https://www.dotforce.es/criptografia-post-cuantica/

[38] https://www.fundacionbankinter.org/noticias/criptografia-post-cuantica/

https://observatorioblockchain.com/ciberseguridad/tendencias-ciberseguridad-2024-criptografia-postcuantica-e-ia/

https://keepcoding.io/blog/que-es-la-criptografia-postcuantica/

https://digital-strategy.ec.europa.eu/es/news/commission-publishes-recommendation-post-quantum-cryptography

https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

https://www.technologyreview.es/s/11310/que-es-la-criptografia-poscuantica-y-por-que-se-volvera-impresdincible

[39] https://cso.computerworld.es/cibercrimen/la-amenaza-cuantica-la-computacion-cuantica-y-la-criptografia

https://www.farodevigo.es/tendencias21/2024/01/03/ordenadores-cuanticos-romper-internet-decada-96486818.html

https://www.levante-emv.com/tendencias21/2024/01/03/ordenadores-cuanticos-romper-internet-decada-96486790.html

https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers

https://grupooesia.com/insight/criptografia-cuantica-y-su-impacto-en-nuestra-ciberseguridad/

[40] https://www.bbc.com/mundo/noticias-60141571

https://www.technologyreview.es/s/11209/un-ordenador-cuantico-rompera-el-cifrado-rsa-de-2048-bits-en-ocho-horas

https://www.levante-emv.com/tendencias21/2024/01/03/ordenadores-cuanticos-romper-internet-decada-96486790.html

[41] https://www.universidadviu.com/es/actualidad/nuestros-expertos/que-es-la-criptografia-y-cuales-son-sus-usos

https://www.nationalgeographic.com.es/ciencia/criptografia-ciencia-que-protege-era-digital_21781

https://blog.internxt.com/es/que-es-la-criptografia/

https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines

https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends

https://ieeexplore.ieee.org/document/8637988/references#references

https://www.hhs.gov/sites/default/files/quantum-cryptography-and-health-sector.pdf

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175Br1.pdf

https://www.enisa.europa.eu/publications/the-use-of-cryptographic-techniques-in-europe/@@download/fullReport

https://www.csl.sri.com/papers/vcdm-did-crypto-recs/crypto-review-and-recs-for-VCDM-and-DIDs-implems-FINAL-20211015.pdf

[42] https://observatorioblockchain.com/ciberseguridad/tendencias-ciberseguridad-2024-criptografia-postcuantica-e-ia/

[43] https://www.muylinux.com/2024/02/13/the-linux-foundation-criptografia-poscuantica/

https://www.lavanguardia.com/vida/formacion/20221216/8647676/victor-gayoso-medio-plazo-desarrollaran-ordenadores-cuanticos-capaces-romper-sistemas-criptograficos-utilizados-actualmente-mkt-emg.html

https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/quantum-safe-encryption

https://www.ibm.com/downloads/cas/EZEGKEB5

[44] https://techiescience.com/es/friction-in-quantum-computing/

[45] https://www.technologyreview.es/s/14985/no-solo-cubits-los-desafios-de-la-computacion-cuantica-en-2023

[46] https://www.xataka.com/investigacion/esta-gran-promesa-computacion-cuantica-millon-cubits-correccion-errores-durante-esta-decada
https://www.xataka.com/investigacion/computacion-cuantica-controlar-cubits-desafio-enorme-esta-innovacion-promete-ser-capaz-dominar-cuatro-millones-plumazo

[47] https://blogthinkbig.com/radiografia-computacion-cuantica
[48] : https://blogthinkbig.com/radiografia-computacion-cuantica

https://arstechnica.com/science/2024/01/quantum-computing-startup-says-it-will-beat-ibm-to-error-correction/

https://www.ibm.com/quantum/blog/error-correction-codes

https://www.xataka.com/investigacion/computacion-cuantica-acalla-criticas-rozamos-correccion-errores-uno-sus-mayores-retos-punta-dedos

https://www.xataka.com/investigacion/algun-dia-se-construye-ordenador-cuantico-plenamente-funcional-sera-gracias-parte-a-este-cientifico-espanol-hablamos-ignacio-cirac-1

https://www.xataka.com/ordenadores/ibm-esta-cumpliendo-su-promesa-sigue-escalando-cubits-asi-crucial-correccion-errores-llegara-pronto

[49] https://www.xataka.com/investigacion/algun-dia-se-construye-ordenador-cuantico-plenamente-funcional-sera-gracias-parte-a-este-cientifico-espanol-hablamos-ignacio-cirac-1

https://qudev.phys.ethz.ch/static/content/courses/phys4/studentspresentations/iontraps/CiracZoller1995.pdf

https://www.xataka.com/ordenadores/dificilisimo-programar-ordenador-cuantico-para-ejecutar-algoritmo-cuantico-solucion-mit-gloriosa

[50] https://digital-strategy.ec.europa.eu/es/policies/quantum

https://digital-strategy.ec.europa.eu/es/news/commission-publishes-recommendation-post-quantum-cryptography

[51] https://www.xataka.com/investigacion/algun-dia-se-construye-ordenador-cuantico-plenamente-funcional-sera-gracias-parte-a-este-cientifico-espanol-hablamos-ignacio-cirac-1

https://qudev.phys.ethz.ch/static/content/courses/phys4/studentspresentations/iontraps/CiracZoller1995.pdf

https://www.mpg.de/371987/quantenoptik_wissM

[52] Vídeo explicativo sobre el qubit https://youtu.be/ilPfvMEOmCs?t=124

Artículo que describe la esfera de Bloch https://medium.com/quantum-untangled/quantum-states-and-the-bloch-sphere-9f3c0c445ea3

Algunas webs interactivas para entender la esfera de Bloch:

https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/blochsphere/blochsphere.html

https://bloch.kherb.io/

https://bits-and-electrons.github.io/bloch-sphere-simulator/#{%22blochSphereStateProperties%22:{%22theta%22:%220.0000%22,%22phi%22:%2290.0000%22},%22customGatesProperties%22:{},%22lambdaGatesProperties%22:{%22polarAngle%22:%220%22,%22azimuthAngle%22:%220%22}}

[53] https://www.researchgate.net/publication/339971232_The_Road_to_Quantum_Computational_Supremacy

https://journals.aps.org/pr/abstract/10.1103/PhysRev.47.777

https://journals.aps.org/pr/pdf/10.1103/PhysRev.47.777

"The Quest for Quantum Supremacy: A Roadmap for NISQ Devices" by Preskill, John (2020):

Ese artículo de la revista Physics Today de la American Physical Society analiza la búsqueda de la supremacía cuántica y el papel de la dualidad onda-partícula de la luz en la informática cuántica. Hace referencia a las contribuciones de Planck, Einstein y Young.

[54] "Quantum **Computation and Quantum Information"** por Nielsen, Michael A. y Chuang, Isaac L. (2000) https://profmcruz.wordpress.com/wp-content/uploads/2017/08/quantum-computation-and-quantum-information-nielsen-chuang.pdf

https://www.academia.edu/41154803/Quantum_Computation_and_Quantum_Information_by_Nielsen_and_Chuang

"Quantum Computing: A Primer" por Mermin, N. David (2020)

"The Quest for Quantum Supremacy: A Roadmap for NISQ Devices" por Preskill, John (2020)

[55] https://learn.microsoft.com/es-es/ai/playbook/technology-guidance/generative-ai/working-with-llms/

https://blogs.microsoft.com/blog/2023/09/21/announcing-microsoft-copilot-your-everyday-ai-companion/

https://blog.google/technology/ai/lamda/

https://developers.google.com/machine-learning/resources/intro-llms?hl=es-419

[56] https://gemini.google.com/

[57] www.ibm.com/thought-leadership/institute-business-value/en-us/report/quantum-safe-encryption

[58]

https://www.ibm.com/downloads/cas/EZEGKEB5

https://www.ibm.com/think/quantum

https://www.ibm.com/thought-leadership/institute-business-value/technology/quantum-computing

https://newsroom.ibm.com/2022-05-10-IBM-Unveils-New-Roadmap-to-Practical-Quantum-Computing-Era-Plans-to-Deliver-4,000-Qubit-System

https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/quantum-safe-encryption

[59] https://www.youtube.com/watch?v=bfYH7JmHQnk

[60] https://youtu.be/mVu_kOtuybM?t=164

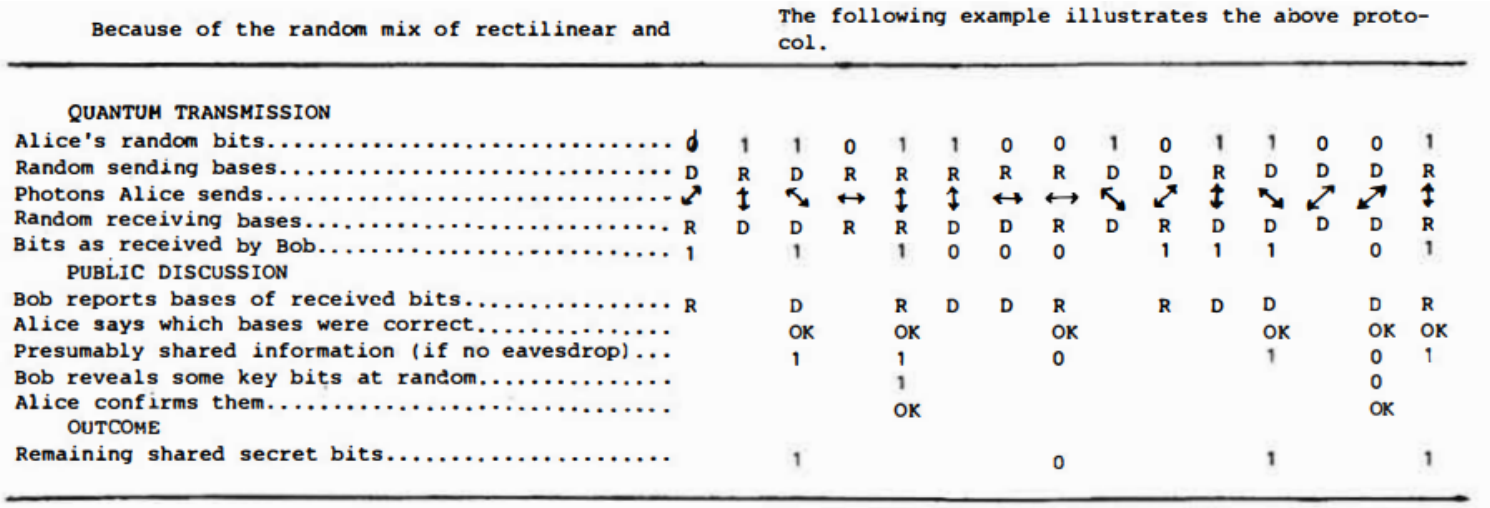
[61] https://www.youtube.com/watch?v=xLL6ly830dA

[62] https://youtu.be/IrUPkZ8oBhw?t=141

[63] https://oa.upm.es/1298/1/PFC_JESUS_MARTINEZ_MATEO.pdf página 21

https://arxiv.org/abs/2003.06557

https://arxiv.org/pdf/2003.06557



Because of the random mix of rectilinear and

The following example illustrates the above protocol.

QUANTUM TRANSMISSION														
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	↗	↕	↘	↔	↕	↕	↔	↔	↘	↗	↕	↘	↗	↗	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

https://web.archive.org/web/20231118012846/http://oa.upm.es/1298/1/PFC_JESUS_MARTINEZ_MATEO.pdf

[64] https://arxiv.org/html/2403.02240v1#S4 ver punto 4.2

[64 – 1] D. J. Bernstein and T. Lange, "Post-quantum cryptography," Nature, vol. 549, no. 7671, pp. 188–194, 2017.

Estas referencias 1, 2 y 3 derivadas de la 64, son las referencias originales del texto referenciado en internet, para no tener que estar subiendo y bajando a ellas constantemente según éste es leído.

[64 – 2] A. Kumar et al., "Securing the future internet of things with post-quantum cryptography," Security and Privacy, vol. 5, no. 2, p. e200, 2022

[64 – 3] C. R. García, S. Rommel, S. Takarabt, J. J. V. Olmos, S. Guilley, P. Nguyen, and I. T. Monroy, "Quantum-resistant transport layer security," Computer Communications, vol. 213, pp. 345–358, 2024

[65] https://youtu.be/YpYuBEzfRlM?t=214

[66] referencia sobre qué son los números complejos, explicado por el matemático Eduardo Sáenz de Cabezón: https://www.youtube.com/watch?v=LqyBrrgmIro

[Imagen 1]

Table 1: Examples of most commonly used cryptographic systems and their resistance to quantum attacks.[3]

Cryptography standard (in-use)	Function	Post-quantum security level	Examples of today's use
RSA-2048	Encryption & signature	Broken	Internet traffic, including the webpages of all European Institutions, banks, energy, and transport companies.
RSA-3072	Encryption & signature	Broken	VPNs, financial transactions, minimum security level required for intelligence secrets, e-passports.
DH-3072	Key exchange	Broken	Internet protocols such as SSL/TLS, SSH, and IPSec.
256-bit ECDSA	Signature	Broken	Used in Bitcoin and Ethereum exchanges, Companies' internal communications.

All cryptography algorithms in this table were also listed as vulnerable by the White House in the November 2022 migration memorandum - examples of use retrieved by the author.

4

Otros estudios sobre cómo funciona la cuántica:

https://drrajivdesaimd.com/2020/04/12/quantum-computing/

https://medium.com/aiguys/overview-on-quantum-computing-2b1ce1407fe2

https://www.connectedpapers.com/main/54d2fc4cb94a64f972ff8dc9e80670882f42e749/Quantum-Computing-and-its-Impact-on-Cryptography/graph

https://www.connectedpapers.com/main/239bf45c13b3f6d38c74026b535f785febf9cd08/Towards-Post%20Quantum-Blockchain%3A-A-Review-on-Blockchain-Cryptography-Resistant-to-Quantum-Computing-Attacks/graph

[67] https://youtu.be/FL8wNX661Gw?t=1081

[68] https://qutech.nl/ página web oficial de QuTech, el instituto de investigación para la computación cuántica y el internet cuántico de Países Bajos, en Europa.

[69] Esta es probablemente la referencia más importante y relevante de este TFG

https://www.ibm.com/es-es/topics/quantum-cryptography

https://web.archive.org/web/20240712183543/https://www.ibm.com/es-es/topics/quantum-cryptography

[70] https://hipertextual.com/2016/09/d-wave-google-nasa

Estas son algunas capturas del TFG de Jesús Martínez Mateo, que constantan la nula probabilidad de que, en los datos procesados en la cuántica, se pueda duplicar un estado. Luego en un sistema como este, jamás se podría falsificar información duplicándola. [63]

A.2. Demostraciones

Teorema de no-clonación

Podemos realizar una demostración simple del teorema de no-clonación probando que no existe ninguna operación unitaria, U, que permita la evolución: $\psi \otimes |0\rangle \rightarrow \psi \otimes \psi$, para cualquier estado, ψ. Para ello, partimos del supuesto de que dicha operación unitaria existe, e intentamos clonar los estados $|0\rangle$ y $|1\rangle$, luego existe:

$$U\,|0\rangle \otimes |0\rangle = |0\rangle \otimes |0\rangle$$

$$U\,|1\rangle \otimes |0\rangle = |1\rangle \otimes |1\rangle$$

Y puesto que trabajamos sobre un sistema lineal, tenemos que:

$$U\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$$

Que no coincide con el resultado esperado de una clonación, $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

La ecuación representa una operación cuántica, específicamente la **puerta Hadamard**, aplicada a un estado cuántico. La puerta Hadamard es una de las puertas básicas utilizadas en la computación cuántica para crear estados de superposición. Vamos a desglosarla:

1. **Operador Unitario (U):** El símbolo (U) representa la operación que se realiza sobre un estado inicial.
2. **Estado Inicial (|(-\rangle)):** El estado inicial es (|(-\rangle)), que es uno de los estados base en un sistema de un solo qubit. Este estado se encuentra en una superposición igual de los estados 0 y 1: [|(-\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)]
3. **Producto Tensorial (⊗):** El símbolo (\otimes) denota el producto tensorial. En este caso, el estado (|(-\rangle)) se combina con otro qubit en el estado (|0\rangle): [|(-\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |0\rangle)]
4. **Resultado Final:** La expresión completa muestra que aplicar la puerta Hadamard al estado (|(-\rangle)) resulta en un estado entrelazado donde ambos estados base originales son igualmente probables debido a los coeficientes iguales por el factor de normalización.

En resumen, esta ecuación describe cómo un sistema de dos qubits, donde uno de ellos se somete a una transformación Hadamard, resulta en un estado entrelazado donde ambos estados base originales tienen igual probabilidad debido a la normalización.

1. **Enunciado del Teorema:**
    - El objetivo es demostrar que no existe una operación unitaria (U) que permita clonar un estado cuántico arbitrario.
    - Clonar significa crear una copia exacta del estado original.
2. **Supongamos que existe una operación (U) que clona:**
    - Consideremos dos estados cuánticos: (|0\rangle) (estado base) y (|1\rangle).
    - Aplicamos (U) a (|0\rangle) y (|1\rangle):
        - (U |0\rangle = |0\rangle)
        - (U |1\rangle = |1\rangle)
3. **Linealidad y Consistencia:**
    - Dado que trabajamos con un sistema lineal, esperamos que (U) actúe de manera consistente en diferentes estados.
    - Sin embargo, si aplicamos (U) al estado combinado (\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes |\psi\rangle), obtenemos:
        - (U \left(\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)\right) \otimes |\psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle \otimes |\psi\rangle + |1\rangle \otimes |\psi\rangle))

    - Sin embargo, si aplicamos (U) al estado combinado (\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes |\psi\rangle), obtenemos:
        - (U \left(\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)\right) \otimes |\psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle \otimes |\psi\rangle + |1\rangle \otimes |\psi\rangle))

        - Esto **no** coincide con (\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes |\psi\rangle).
4. **Conclusión:**
    - La inconsistencia en la clonación demuestra que no existe una operación (U) que pueda clonar estados cuánticos arbitrarios.

En resumen, el teorema de no clonación es fundamental en la teoría de la información cuántica y tiene aplicaciones en la seguridad de la comunicación cuántica y la computación cuántica. Si tienes más preguntas o

Estilo y formato del TFG

El TFG consistirá en un único documento que deberá cumplir los siguientes requisitos de estilo y forma. **En el caso de que el TFG consista en un trabajo de Investigación, indicamos los siguientes requisitos formales que deben cumplir los alumnos, y que serán evaluados conforme a la rúbrica de evaluación que contiene este documento.**

- Extensión: los trabajos de investigación deberán tener una extensión mínima de 30 páginas (sin contar portada, bibliografía, fotografías, índices ni anexos), no pudiendo exceder las 100 páginas incluidos los anexos y la bibliografía (sin contar portada e índice) sin la autorización expresa del tutor
- Tipo de letra: Times New Roman. Tamaño obligatorio 12 (salvo notas a pie de página: en caso de haberlas, estas tendrán un tamaño de 10 puntos).
- Formato de página: Tamaño A4. Pueden intercalarse páginas verticales y horizontales (apaisadas), estas últimas para presentación de tablas, por ejemplo.
- Interlineado del texto: espacio 1,5 (salvo en el caso del texto en las tablas, en el que puede ser menor).
- Márgenes: Laterales de 2,5 cm y el texto justificado en ambos. Superior 3,5 e inferior 2.
- Encabezado: Se incluirá el título del trabajo, así como nombre y apellidos del alumno.
- Pie de página: Se incluirá la numeración de las páginas del documento.
- Portada o carátula: Todo el texto irá en negrita y centrado. En la portada se harán constar los siguientes datos:

GRADO EN GESTIÓN DE CIBERSEGURIDAD
“Título del trabajo”
Nombre y apellidos del alumno
Curso académico *20XX/20XX*

Universidad Francisco de Vitoria

- Formato de archivo: Se entregará el documento en el Aula virtual, mediante un único archivo en formato PDF.
- Tamaño máximo del archivo: 8 MB.
- Las citas o referencias bibliográficas deberán ajustarse a los criterios de cita de APA. Se adjunta el link a las citadas normas https://normas-apa.org/citas/

Estructura del TFG

A continuación, se incluye **una propuesta de estructura** para que el alumno pueda desarrollar en su TFG. En todo caso, la estructura del trabajo (apartados a incluir, orden de los mismos, etc.) sí deberá ajustarse a la expuesta.

Además, el TFG debe contener:

- Portada. Conforme a lo indicado anteriormente.
- Dedicatoria y agradecimiento (no obligatorio)
- Declaración personal de no plagio. Tras la portada, el alumno deberá incluir la DECLARACIÓN PERSONAL DE NO PLAGIO, incluida en el anexo de este documento, debidamente cumplimentada y firmada.

IMPORTANTE: No serán calificados los TFG de aquellos alumnos que no incluyan correctamente la DECLARACIÓN PERSONAL DE NO PLAGIO.

Es importante definir y relacionar los escritos, documentos, trabajos, encuestas y demás fuentes de información utilizadas en el trabajo, así como distinguirlos claramente las fuentes o los que son de autoría propia. Debe tenerse precaución con copiar textos, sean de documentos editados o de la web u otra fuente, para llevarlos directamente al Trabajo Final, sin citar debidamente las fuentes. Esto se considera plagio y será objeto de penalización. Es decir, ha de quedar claramente reflejado lo que es propio y lo que no. A tal fin se incluyen como anexo las

normas de citado que debe tener en cuenta el alumno a la hora de incluir en su TFG el trabajo de otros autores.

- Índice paginado: Índice de contenidos detallando en el mismo las cuestiones más relevantes tratadas en la resolución del caso.
- Resolución de las cuestiones planteadas en cada caso conforme a las indicaciones incluidas en cada supuesto.
- Conclusiones
- Bibliografía: En la que se incluya bibliografía, las páginas web o cualquier otra documentación en la que el alumno fundamente sus propuestas de resolución
- Anexos: Incluirán aquellos documentos en los que el alumno fundamente, bien su trabajo de investigación o los razonamientos que justifiquen la resolución del caso propuesto.