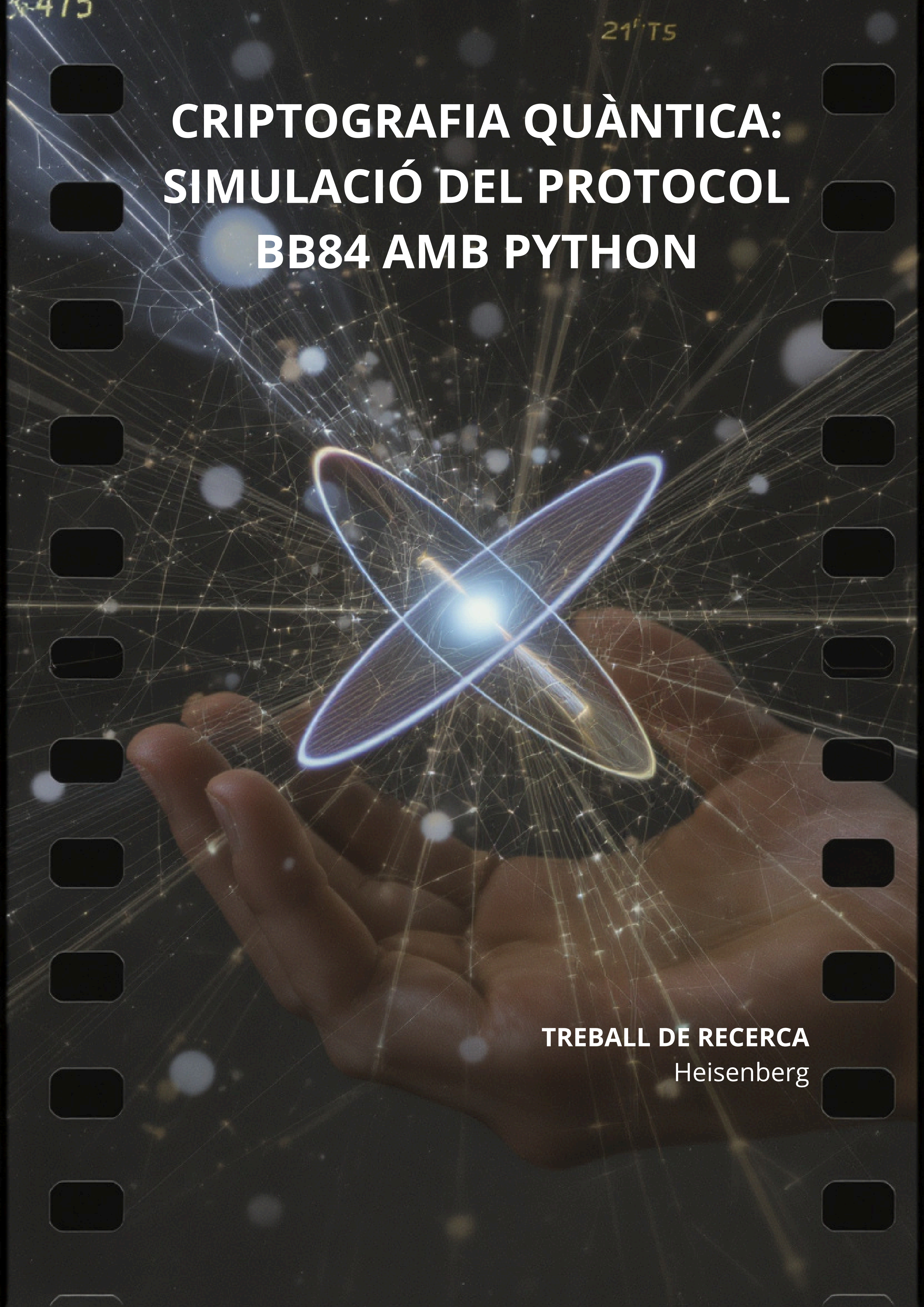


CRIPTOGRAFIA QUÀNTICA: SIMULACIÓ DEL PROTOCOL BB84 AMB PYTHON

TREBALL DE RECERCA
Heisenberg

"La criptografia quàntica pot oferir la seguretat que avui no podem ni imaginar. En el futur, les comunicacions segures poden ser una realitat gràcies a la física quàntica."

Artur Ekert

RESUM

Aquest treball de recerca ofereix una anàlisi exhaustiva dels fonaments de la física quàntica i la seva aplicació pràctica en el camp de la criptografia moderna, centrant-se específicament en el protocol BB84. La hipòtesi principal estableix que mitjançant la simulació computacional d'aquest protocol és possible detectar eficaçment intercepcions en la transmissió de claus quàntiques, ja que qualsevol intent d'espionatge introdueix alteracions mesurables i quantificables en la clau secreta compartida entre els usuaris.

El marc teòric desenvolupat examina en profunditat conceptes quàntics essencials com el principi d'incertesa de *Heisenberg, la superposició d'estats i el fenomen entrellaçament quàntic, tots els pilars fonamentals que garanteixen la seguretat del protocol BB84. Aquests principis físics asseguren que qualsevol mesurament no autoritzat sobre el sistema quàntic modifiqui inevitablement l'estat dels qubits transmesos, deixant així una petjada detectable de l'intent d'intercepció.

La part pràctica es materialitza a través d'una simulació desenvolupada en Python que recrea meticulosament totes les etapes del protocol: des de la generació i codificació dels qubits fins a la seva transmissió, mesurament i posterior processament. El model incorpora de manera realista la possible intercepció per part d'un espia extern, denominat Eva, cosa que permet quantificar l'impacte de les seves accions sobre la integritat de la comunicació.

Els resultats obtinguts a través de múltiples simulacions confirmen contundentment la hipòtesi inicial, demostrant que quan Eva intercepta els qubits transmesos, la taxa d'error en la clau resultant experimenta un increment significatiu i mesurable. El protocol estableix criteris precisos, determinant que si aquesta taxa d'error supera un llindar de l'11%, la clau ha de ser immediatament descartada per considerar-se compromesa. Aquesta recerca evidencia la viabilitat operativa del protocol BB84 per a assegurar comunicacions en entorns hostils, destacant la seva directa dependència de les propietats fonamentals de la mecànica quàntica i la seva

capacitat per a prioritzar la seguretat absoluta sobre consideracions operatives o d'eficiència en la distribució de claus criptogràfiques.

RESUMEN

Este trabajo de investigación ofrece un análisis exhaustivo de los fundamentos de la física cuántica y su aplicación práctica en el campo de la criptografía moderna, centrándose específicamente en el protocolo BB84. La hipótesis principal establece que mediante la simulación computacional de este protocolo es posible detectar eficazmente interceptaciones en la transmisión de claves cuánticas, ya que cualquier intento de espionaje introduce alteraciones medibles y cuantificables en la clave secreta compartida entre los usuarios.

El marco teórico desarrollado examina en profundidad conceptos cuánticos esenciales como el principio de incertidumbre de Heisenberg, la superposición de estados y el fenómeno de entrelazamiento cuántico, todos ellos pilares fundamentales que garantizan la seguridad del protocolo BB84. Estos principios físicos aseguran que cualquier medición no autorizada sobre el sistema cuántico modifique inevitablemente el estado de los qubits transmitidos, dejando así una huella detectable del intento de interceptación.

La parte práctica se materializa a través de una simulación desarrollada en Python que recrea meticulosamente todas las etapas del protocolo: desde la generación y codificación de los qubits hasta su transmisión, medición y posterior procesamiento. El modelo incorpora de manera realista la posible intercepción por parte de un espía externo, denominado Eva, permitiendo cuantificar el impacto de sus acciones sobre la integridad de la comunicación.

Los resultados obtenidos a través de múltiples simulaciones confirman contundentemente la hipótesis inicial, demostrando que cuando Eva intercepta los qubits transmitidos, la tasa de error en la clave resultante experimenta un incremento significativo y medible. El protocolo establece criterios precisos, determinando que si dicha tasa de error supera un umbral del 11%, la clave debe ser inmediatamente descartada por considerarse comprometida. Esta investigación evidencia la viabilidad operativa del protocolo BB84 para asegurar comunicaciones en entornos hostiles, destacando su directa dependencia de las propiedades

fundamentales de la mecánica cuántica y su capacidad para priorizar la seguridad absoluta sobre consideraciones operativas o de eficiencia en la distribución de claves criptográficas.

ABSTRACT

This research paper offers a comprehensive analysis of the fundamentals of quantum physics and its practical application in the field of modern cryptography, focusing specifically on the BB84 protocol. The main hypothesis establishes that by computationally simulating this protocol, it is possible to effectively detect interceptions in the transmission of quantum keys, since any eavesdropping attempt introduces measurable and quantifiable alterations to the secret key shared between users.

The theoretical framework developed examines in depth essential quantum concepts such as the Heisenberg uncertainty principle, the superposition of states, and the quantum entanglement phenomenon, all of which are fundamental pillars that guarantee the security of the BB84 protocol. These physical principles ensure that any unauthorized measurement on the quantum system inevitably modifies the state of the transmitted qubits, thus leaving a detectable trace of the interception attempt.

The practical aspect is realized through a simulation developed in Python that meticulously recreates all stages of the protocol: from the generation and encoding of the qubits to their transmission, measurement, and subsequent processing. The model realistically incorporates the possible interception by an external spy, called Eve, allowing the quantification of the impact of her actions on the integrity of the communication.

The results obtained through multiple simulations strongly confirm the initial hypothesis, demonstrating that when Eve intercepts the transmitted qubits, the error rate in the resulting key experiences a significant and measurable increase. The protocol establishes precise criteria, determining that if the error rate exceeds a threshold of 11%, the key must be immediately discarded as compromised. This research demonstrates the operational viability of the BB84 protocol for securing communications in hostile environments, highlighting its direct dependence on the fundamental properties of quantum mechanics and its ability to prioritize absolute security over operational considerations or efficiency in the distribution of cryptographic keys.

ÍNDEX

INTRODUCCIÓ

La física quàntica, també coneguda com a mecànica quàntica, és una branca de la física que estudia el comportament de la matèria i l'energia molt petites, com les dels àtoms i les partícules subatòmiques. A diferència de la física clàssica, que descriu el món que percebem amb els nostres sentits, la física quàntica revela un univers ple de fenòmens estranys i aparentment contradictoris: partícules que poden estar en diversos llocs alhora, accions que passen instantàniament a distància, i estats que només es defineixen quan són observats.

Aquesta teoria va revolucionar la nostra comprensió del món des del segle XX, amb contribucions clau de científics com Max Planck, Albert Einstein, Niels Bohr i Erwin Schrödinger. Gràcies a la física quàntica, avui dia gaudim de tecnologies com els làsers, els semiconductors i la computació quàntica.

He triat fer aquest treball sobre física quàntica perquè és un tema que em desperta molta curiositat. Tot i que és complex i ple d'idees difícils d'imaginar, també és una de les àrees més fascinants de la ciència. Vull entendre millor com funciona el món a escala microscòpica, descobrir els principis que regeixen l'univers i conèixer les aplicacions tecnològiques que neixen d'aquesta teoria. A més, crec que aprendre sobre física quàntica m'ajudarà a desenvolupar una manera de pensar més lògica, crítica i oberta a noves idees.

Una de les aplicacions més importants i revolucionàries de la física quàntica és la criptografia quàntica, que utilitza les propietats úniques de les partícules quàntiques per garantir la seguretat en la transmissió d'informació. El protocol BB84, desenvolupat l'any 1984 per Charles Bennett i Gilles Brassard, és el primer i un dels més coneguts protocols de distribució de claus quàntiques. Aquest protocol aprofita fenòmens com la superposició i la mesura quàntica per permetre que dos usuaris comparteixin una clau secreta de manera segura, detectant qualsevol intent d'interceptar la comunicació. Així, el BB84 exemplifica com la física quàntica pot oferir solucions innovadores a problemes clàssics, com la protecció de la informació, i obre el camí a noves tecnologies que poden transformar la nostra societat.

HIPÒTESI I OBJECTIUS

Per poder dur a terme el present treball de recerca es planteja la següent hipòtesi: si es duu a terme una simulació del protocol BB84 utilitzant un entorn de programació com Python, amb el suport de biblioteques especialitzades en computació quàntica com QuTiP o Qiskit, és possible detectar qualsevol intent d'intercepció en la transmissió de claus quàntiques. Aquesta detecció es produeix gràcies a l'aparició d'errors en la clau compartida, els quals serien conseqüència directa de la presència d'un espia en el procés de comunicació. La hipòtesi, doncs, planteja que la mateixa naturalesa dels sistemes quàntics i les seves propietats fonamentals permeten identificar de manera inequívoca un atac al canal de transmissió.

Per tal de validar o refutar aquesta hipòtesi s'estableix una sèrie d'objectius concrets que guiaran tot el desenvolupament del treball. En primer lloc, és necessari investigar sobre els inicis i la història de la física quàntica, ja que només a través de la comprensió del context històric i científic en què va sorgir aquests conceptes es pot entendre la seva aplicació actual en camps com la criptografia. En segon lloc, es proposa aprofundir en els principis bàsics del protocol BB84, analitzant tant la seva formulació original com les diferents implementacions que se n'han fet dins l'àmbit de la criptografia quàntica, per tal de comprendre per què és considerat el primer i un dels més segurs protocols de distribució de claus.

En tercer lloc, cal familiaritzar-se amb el llenguatge de programació Python i amb biblioteques específiques com QuTiP i Qiskit, que permeten simular processos quàntics en un entorn computacional clàssic. L'ús d'aquestes eines és essencial per poder dur a terme una simulació fidel al comportament real dels qubits i de les seves interaccions. En quart lloc, s'ha de desenvolupar una simulació funcional del protocol BB84 que permeti reproduir pas a pas la transmissió d'una clau quàntica entre dos usuaris, anomenats habitualment l'Alícia i el Bob, i que incorpori les fases de preparació, transmissió, mesura i filtratge de bits.

En cinquè lloc, es planteja introduir un possible atac o intercepció dins la simulació, representant per la figura d'un espia anomenat Eva, i analitzar de manera detallada com aquesta intervenció afecta la clau final compartida. L'objectiu és observar si, tal com preveu la teoria, els errors augmenten de manera significativa en presència de l'espionatge. Finalment, mitjançant aquesta anàlisi comparativa, es pretén validar o refutar la hipòtesi inicial demostrant de manera pràctica la capacitat del protocol BB84 de detectar intents d'atac gràcies a l'aparició d'errors estadísticament mesurables en la clau compartida.

La metodologia emprada en el desenvolupament del treball és de caràcter inductiu, ja que parteix de l'observació i de l'experimentació com a instruments principals per arribar a conclusions. Així, a través de la implementació de simulacions, de l'anàlisi dels resultats obtinguts i de la interpretació de les dades, es busca confirmar o bé refutar la hipòtesi inicial. Aquesta aproximació permet no només comprovar si la teoria es compleix en la pràctica, sinó també adquirir una visió crítica sobre els límits i les possibilitats del protocol BB84 i de les tecnologies quàntiques aplicades a la seguretat de la informació.

MARC TEÒRIC

1. Conceptes bàsics i introducció a la física quàntica

1.1 Què és la mecànica quàntica i per què és important?

La mecànica quàntica és la branca de la física que estudia el comportament de la matèria i l'energia a escales molt petites, principalment a nivells d'àtoms i partícules subatòmiques com a electrons, protons, neutrons, fotons, etc. A diferència de la física clàssica, que descriu el món a gran escala (com a planetes o cotxes), la mecànica quàntica explica fenòmens que no poden entendre's amb les lleis clàssiques.

La importància de la mecànica quàntica radica en el fet que ha revolucionat la nostra comprensió de l'univers. Gràcies a ella, entenem per què els àtoms són estables, com funcionen els semiconductors (són materials amb una banda prohibida intermèdia que permet controlar la seva conductivitat mitjançant dopatge i estímuls externs i la base de l'electrònica moderna), com es produeix la llum làser, com ocorre la fusió nuclear en les estrelles i molts altres fenòmens. A més, la mecànica quàntica ha donat lloc a tecnologies com la ressonància magnètica, la computació quàntica i la criptografia quàntica, que estan transformant la ciència i la societat.[1] [2] [3]

1.2 Diferències entre la física clàssica i la quàntica

En la física clàssica, ens movem en el món macroscòpic (planetes, cotxes, projectils), on les lleis de Newton i Maxwell permeten predir amb certesa el futur d'un sistema si coneixem les seves condicions inicials (posició, velocitat, forces). Les magnituds físiques (energia, posició, velocitat) varien de manera contínua i no existeix cap limitació fonamental en la precisió amb la qual podem mesurar-les. Observar un objecte, per exemple, mesurar la velocitat d'un automòbil, no altera el

[1] Coluccio Leskow, Estefania. *Mecánica cuántica* [en línia]. Enciclopedia Concepto, 24 d'octubre de 2024 [Consultat: 22 d'abril de 2025]. Disponible a: https://concepto.de/mecanica-cuantica/
[2] Planas, Oriol. *Física quàntica: què és i principis de la mecànica quàntica* [en línia]. Energia Nuclear, 21 de juny de 2023 [Consultat: 22 d'abril de 2025]. Disponible a: https://ca.energia-nuclear.net/fisica/quantica
[3] Escuela PCE. *Resumen de la mecánica cuántica* [en línia]. Escuela PCE, data no disponible [Consultat: 22 d'abril de 2025]. Disponible a: https://escuelapce.com/resumen-de-la-mecanica-cuantica/

seu estat de forma apreciable. A més, les entitats es classifiquen clarament com a ones (ones de so, ones en l'aigua) o com a partícules (boles, planetes), sense solapament entre totes dues naturaleses.

En canvi, la mecànica quàntica descriu el món molt petit, àtoms, electrons, fotons… on tots aquests conceptes canvien radicalment:

1. **El determinisme deixa pas a la probabilitat**. Ja no parlem de trajectòries definides, sinó de "funcions d'ona" que assignen probabilitats als possibles resultats d'un mesurament. Només en observar col·lapsa aquesta funció i es tria un sol valor.
2. **Les magnituds estan quantitzades**. No poden prendre qualsevol valor, sinó únicament uns certs nivells discrets o "quants", com els electrons, on només ocupen òrbites atòmiques amb energies fixes.
3. **Onda i partícules es fusionen.** Un mateix objecte quàntic pot comportar-se com a ona, interferint amb si mateix, o com a partícula, localitzant-se en un punt quan el detectem, segons mostri l'experiment, com en la doble escletxa.
4. **Existeix un límit en la precisió del mesurament:** el principio d'incertesa de Heisenberg, estableix que no és possible conèixer simultàniament la posició i el moment lineal d'una partícula amb exactitud arbitrària, com més precís sigui un d'ells, més incert queda l'altre.
5. **L'observació altera el sistema.** En quàntica, l'acte de mesurar modifica l'estat del sistema, una cosa insòlita en la física clàssica.[4]

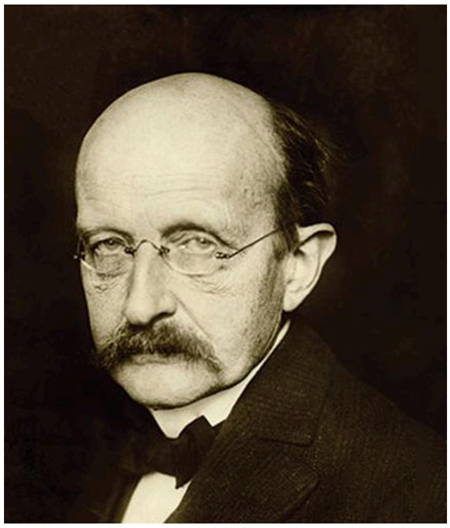
1.3 Història de la física quàntica: Des de Planck fins a l'actualitat.

La física quàntica va néixer l'any 1900 quan Max Planck va proposar que l'energia no s'emet de manera contínua, sinó en paquets discrets anomenats quants, per tal d'explicar l'espectre de radiació del cos negre. Aquesta idea revolucionària va

[4] La Reserva. *Comprendiendo las diferencias entre la física clásica y la física cuántica* [en línia]. La Reserva, 13 de juny de 2023 [Consultat: 22 d'abril de 2025]. Disponible a: https://www.lareserva.com/diferencias_entre_fisica_clasica_y_fisica_cuantica

trencar amb la noció clàssica de l’energia com un flux continu i va establir la base per a la nova teoria (Kragh, 2000).[5] [6]

Pocs anys després, el 1905, Albert Einstein va aplicar el concepte de quants a la llum per interpretar l’efecte fotoelèctric, demostrant que la llum podia comportar-se com a partícula (fotó) i no només com a ona. Aquest descobriment no només va validar la hipòtesi de Planck, sinó que també va introduir la idea de la dualitat ona-partícula.[7]



Imatge 1. Max Planck, el Mesías de la física cuántica
Extreta de: https://invdes.com.mx/ciencia-ms/max-planck-mesias-la-fisica-cuantica/

Durant les dècades següents, diversos científics van completar el marc teòric:

- Niels Bohr (1913) va formular el seu model atòmic, en el qual els electrons orbiten el nucli en nivells d’energia quantitzats.
- Werner Heisenberg (1927) va enunciar el principi d’incertesa, establint un límit fonamental a la precisió amb què es poden mesurar simultàniament la posició i el moment d’una partícula.
- Erwin Schrödinger (1926) va desenvolupar l’equació que porta el seu nom, capaç de predir l’evolució temporal de la funció d'ona d’un sistema quàntic.

Imatge 2. Werner Heisenberg
Extreta de: https://ca.wikipedia.org/wiki/Werner_Heisenberg

A mitjans del segle XX, la interpretació de Copenhaguen (Bohr, Heisenberg) va consolidar la visió probabilista de la mesura quàntica i el col·lapse de la funció d’ona davant l’observació. Des de llavors, la física quàntica ha continuat avançant:

[5] Kragh, H. (2000). *Quantum generations: A history of physics in the twentieth century*. Princeton University Press.
[6] BBC News Mundo. *Max Planck, el padre de la teoría cuántica que intentó convencer a Hitler de que permitiera trabajar a los científicos judíos* [en línia]. BBC News Mundo, 23 d’abril de 2019 [Consultat: 30 d’abril de 2025]. Disponible a: https://www.bbc.com/mundo/noticias-48025060
[7] Latorre, J. I. (2017).*Cuántica: Tu futuro en juego*. *Editorial Ariel*

- **Computació quàntica:** utilitza qubits que exploten la superposició i l'entrellaçament per resoldre problemes inabastables per als ordinadors clàssics.
- **Criptografia quàntica:** garanteix comunicacions perfectament segures basades en les propietats essencials de la mesura quàntica.
- **Experiments de gran posició:** com els rellotges atòmics i la interferometria de matèria, que posen a prova les prediccions més fines de la teoria.

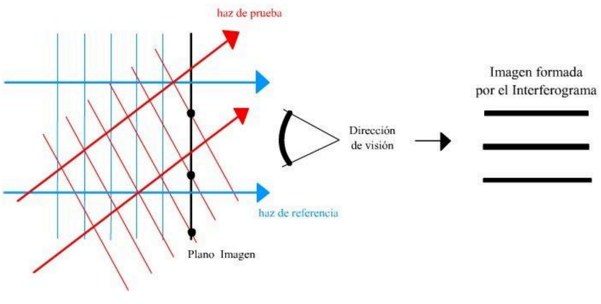
1.4 Dualitat ona-partícula: Com pot la llum ser ona i partícula alhora.

La dualitat ona-partícula és un dels conceptes més sorprenents de la física quàntica, ja que trenca amb la idea clàssica que alguna cosa ha de ser o bé ona o bé partícula. En realitat, la llum, i qualsevol partícula quàntica, és un sistema quàntic que pot manifestar propietats de tots dos segons el tipus d'experiment que realitzem. Com va demostrar l'experiment de la doble escletxa, el comportament ondulatori o corpuscular de les partícules depèn del context de l'observació (Feynman, Leighton, & Sands, 1965)[8]. A continuació les seves cares principals.[9][10]

1.4.1 Comportament ondulatori

- **Interferència i difracció.**

  En fer passar un feix de llum per dues escletxes molt properes (experiment que va fer Thomas Young), observem a la pantalla un patró de franges clares i fosques. Aquestes franges només s'expliquen si considerem la llum com una ona: els vents de les ones que surten de cada escletxa es reforcen mútuament en



Imatge 3. Researchgate
Extreta de:
https://www.researchgate.net/figure/Figura-35-Definicion-de-un-patron-de-interferencia-Diagrama-que-muestra-los-frentes-de_fig13_232659236

[8] Feynman, R. P., Leighton, R. B., & Sands, M. (1965). *The Feynman Lectures on Physics, Vol. 3: Quantum Mechanics*. Addison-Wesley.
[9] Pais, A. (04/06/2020). *Física cuántica: qué es la dualidad partícula-onda de la luz y cómo su descubrimiento revolucionó la ciencia. https://www.bbc.com/mundo/noticias-52815076*
[10] Wikipedia. *Dualidad onda corpúsculo* [en línia]. Wikipedia, data no disponible [Consultat: 24 d'abril de 2025]. Disponible a: https://es.wikipedia.org/wiki/Dualidad_onda_corp%C3%BAsculo

alguns punt (màxims d'interferència) i s'anul·len en altres (mínims).[11]

- **Longitud d'ona i coherència**
  La capacitat de la llum per produir fenòmens de difracció (com corbar-se en passar per un obstacle), depèn de la seva longitud d'ona. Aquest comportament és típic d'ones i no tindria sentit si la llum fossin només partícules clàssiques.

1.4.2 Comportament corpuscular

- **Efecte fotoelèctric**
  Quan la llum incideix sobre la superfície d'un metall, només els fotons amb una energia mínima, poden arrancar electrons. Aquest resultat mostra que l'energia de la llum no és contínua, sinó que ve en "paquets", és a dir, quants, de valor **E=hv,** on la "E" representa l'energia d'un fotó, la "v" representa la freqüència de l'ona electromagnètica corresponent al fotó i per últim la "h" seria la constant de Planck, que es aproximadament $6{,}626 \times 10^{-34}$ J·s. Cap teoria d'ones clàssiques podia predir que disminuir la intensitat lumínica, impediria l'emissió d'electrons.
- **Detecció discreta**
  En mesurar la llum amb detectors sensibles, aquesta apareix com un flux d'impactes individuals: cada fotó arriba en un instant concret i diposita la seva energia de cop.

1.4.3 Principi de complementarietat

Niels Bohr va proposar que ona i partícula són complementàries: no podem observar simultàniament ambdues propietats en un mateix experiment. El disseny experimental determina quin aspecte es revela. Aquesta idea es coneix com el principi de complementarietat, i és fonamental per entendre la interpretació de Copenhaguen de la física quàntica (Bohr, 1928)[12].

- Si configurem l'experiment per mesurar patrons d'interferència, la llum es comporta com una ona.

---

[11] Wikipedia. *Dualidad onda corpúsculo* [en línia]. Wikipedia, data no disponible [Consultat: 24 d'abril de 2025]. Disponible a: https://es.wikipedia.org/wiki/Dualidad_onda_corp%C3%BAsculo
[12] Bohr, N. (1928). The quantum postulate and the recent development of atomic theory. *Nature*, *121*(3050), 580–590.

- Si estem pendents d'impactes individuals o de l'efecte fotoelèctric, la llum es comporta com una partícula.

La llum és un ésser quàntic que traspassa aquestes categories i només adopta una faceta o l'altra.

1.4.4 Implicacions i extensió a la matèria

$$\lambda = \frac{h}{p}$$

Imatge 4. Comportamiento ondulatorio de partículas
Extreta de: https://www.famaf.unc.edu.ar/~gcas/cuantica1/clases/node5.html

Louis de Broglie va ampliar aquesta idea el 1924, proposant que totes les partícules materials (electrons, protons, fotons…) també tenen una longitud d'ona associada.

La "h" es la constant de Planck i la "p" seria el moment lineal, descriu el moviment d'un objecte (N·s)[13][14]

1.5 Superposició quàntica

La superposició quàntica és un principi fonamental de la física quàntica que estableix que una partícula pot existir en múltiples estats al mateix temps fins que es realitza una mesura. A diferència de la física clàssica, on els objectes tenen propietats definides com la posició o la velocitat, en el món quàntic les partícules poden estar en una "barreja" d'estats possibles.

Per exemple, un electró pot estar en dues posicions alhora, o un fotó pot comportar-se com ona i com partícula simultàniament. Només quan es mesura, el sistema "col·lapsa" a un únic estat observable.[15]

A més a més, la superposició se sustenta en els següents principis claus:

- **Combinacions lineals d'estats:** L'estat d'un sistema es descriu mitjançant una funció d'ona, que és una combinació matemàtica (superposició) de tots els estats possibles. Un electró pot estar en dos estats diferents (*ψA o ψB)* el

---

[13] Wikipedia. (27/08/25). *Dualidad onda corpúsculo. https://es.wikipedia.org/wiki/Dualidad_onda_corp%C3%BAsculo*

[14] Martínez, E. (31/07/2025). *La luz tiene dos identidades, pero es imposible verlas a la vez. https://www.levante-emv.com/tendencias21/2025/07/31/luz-identidades-imposible-verlas-vez-120229002.html*

[15] Wikipedia. *Superposició quàntica* [en línia]. Wikipedia, data no disponible [Consultat: 27 d'Abril de 2025]. Disponible a: https://ca.wikipedia.org/wiki/Superposici%C3%B3_qu%C3%A0ntica

seu estat general serà: $\psi = cA\ \psi A + cB\ \psi B$, on cA i cB són coeficients que determinen la probabilitat de cada estat[16]

- **Probabilitat, no certesa:** $|cA|^2$, $|cB|^2$ indica la probabilitat de mesurar cada estat. Per exemple, si un electró està en una superposició de dues posicions, hi ha un 50% de possibilitats de trobar-lo a cadascuna.
- **Col·lapse de la funció d'ona:** En mesurar, la superposició desapareix i el sistema adopta un únic estat definit. Aquest procés és irreversible i aleatori.

Alguns experiments claus on es posen a prova la superposició serien la doble escletxa i el gat de Schrödinger que més endavant parlaré d'ells.[17]

2. Principis i conceptes claus

2.1 Principi d'incertesa d'Heisenberg

Formulat per Werner Heisenberg el 1927, aquest principi estableix que és impossible conèixer simultàniament i amb precisió absoluta dues propietats complementàries d'una mateixa partícula, per exemple la seva posició (x) i el seu moment lineal. La fórmula que expressa aquest principi és:[18]

$$\Delta x\ \Delta p \geq \frac{\hbar}{2}$$

Imatge 5: Why Don't We See the Heisenberg Uncertainty Principle in the Everyday World?
Extreta de: https://www.azoquantum.com/Article.aspx?ArticleID=261

- **Δx** és la incertesa (o dispersió) en la mesura de la posició
- **Δp** és la incertesa en la mesura del moment lineal

[16] Acadèmia EITCA. *Quin és el concepte de superposició en mecànica quàntica i com es relaciona amb el comportament dels qubits en un sistema de N-qubits?* [en línia]. Acadèmia EITCA, 6 d'agost de 2023 [Consultat: 27 d'Abril de 2025]. Disponible a: https://n9.cl/tark7k
[17] *Ibidem*
[18] Sánchez Cuevas, Gema; Sabater, Valeria. *El principi d'incertesa de Heisenberg* [en línia]. La Mente es Maravillosa, 23 de desembre de 2018 [Consultat: 27 d'abril de 2025]. Disponible a: https://lamenteesmaravillosa.com/el-principio-de-incertidumbre-de-heisenberg/

- $\hbar$ és la constant de Planck reduïda (1,05 x 10^{-34} J·s).

Aquest principi va transformar la manera com entenem la naturalesa de les mesures en física quàntica (Heisenberg, 1927).[19]

Quan parlem d'una posició i/o moment, parlem que tenen unes propietats addicionals, no podem afinar al màxim en ambdues alhora. En el cas de fer un experiment podríem arribar a observar que mesurant la posició amb exactitud (Δx molt petit), automàticament la incertesa en el moment lineal (Δp), s'engrandeix, i viceversa. No té un límit tecnològic, no prové de la imperfecció dels nostres instruments, sinó de la mateixa naturalesa quàntica de la matèria. No hi ha cap aparell teòric capaç de vèncer aquest límit. Gràcies a la incertesa, un electró dins un àtom no pot tenir alhora posició i velocitat totalment definides. Si l'electró intentés estar "quiet" al voltant del nucli ($\Delta p=0$), la seva posició (Δx) seria infinita, i no estaria confinat. Aquesta "vibració inevitable" impedeix que l'electró caigui al nucli, garantint que la matèria sigui estable.[20]

2.2 Erwin Schrödinger

Erwin Schrödinger de nom complet Erwin Rudolf Josef Alexander Schrödinger va néixer el 12 d'agost de 1887 a Viena, Àustria. Va estudiar a la Universitat de Viena on va obtenir el doctorat investigant la termodinàmica i l'electrodinàmica.[21]
Durant el seu llegat va fer diferents aportacions com:

1. **Mecànica ondulatòria (1926):** Va introduir la idea de descriure partícules mitjançant funcions d'ona, oferint una alternativa contínua i equivalent a la mecànica matricial d'Heisenberg.
2. **Equació de Schrödinger:** Va formular l'equació temporal de qualsevol sistema quàntic.[22]

---

[19] Heisenberg, W. (1927). Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Zeitschrift für Physik*, *43*(3–4), 172–198.
[20] Wikipedia. *Principi d'incertesa de Heisenberg* [en línia]. Wikipedia, data no disponible [Consultat: 27 d'abril de 2025]. Disponible a: https://ca.wikipedia.org/wiki/Principi_d'incertesa_de_Heisenberg
[21] Wikipedia. *Erwin Schrödinger* [en línia]. Wikipedia, data no disponible [Consultat: 27 d'abril de 2025]. Disponible a: https://es.wikipedia.org/wiki/Erwin_Schr%C3%B6dinger
[22] María, Francisco. *Biografía y contribuciones de Edwin Schrödinger a la física cuántica* [en línia]. OK Diario, 21 de maig de 2025 [Consultat: 30 de Maig 2025]. Disponible a: https://okdiario.com/ciencia/biografia-contribuciones-edwin-schrodinger-fisica-cuantica-14799161

3. **Equivalència amb la mecànica matricial:** Va demostrar que el seu enfocament ondulatori i la teoria de matrius d'Heisenberg són matemàticament equivalents.
4. **Interpretacions de la funció d'ona:** Tot i ser reticent davant la lectura probabilista de Born, les seves discussions van inspirar el debat sobre la naturalesa de la realitat quàntica.

Com s'ha dit l'equació de Schrödinger és l'eina fonamental de la mecànica quàntica: permet calcular com evoluciona en el temps l'estat de qualsevol sistema quàntic i determinar-ne els nivells d'energia. A partir d'això es creen dues equacions depenent de si el temps es dependent o independent:

$$H\Psi = i\hbar\frac{\partial\Psi}{\partial t}$$

Equació dependent del temps

$$\frac{-\hbar^2}{2m}\frac{\partial^2\Psi}{\partial x^2} + U(x)\Psi(x) = E\Psi(x)$$

Equació independent del temps

Imatge 6: Equació de Schrödinger
Extreta de: http://hyperphysics.phy-astr.gsu.edu/hbasees/quantum/Scheq.html

Constitueix la base de la mecànica quàntica i descriu l'evolució temporal de la funció d'ona, que conté tota la informació sobre un sistema microscòpic. A través d'aquesta llei, podem calcular els nivells d'energia d'àtoms, molècules i cristalls, explicant amb precisió espectres d'emissió i absorció i permetent dissenyar dispositius semiconductors. La interpretació probabilista de la funció d'ona (Ψ), on $|\Psi|^2$, és la probabilitat de trobar la partícula en un punt.

Aquest marc matemàtic també serveix per desenvolupar qubits en ordinadors quàntics i cavitats per a làsers, ja que defineix la coherència i la dinàmica dels estats quàntics. A més, s'aplica en la investigació de materials avançats, on la forma de la funció d'ona determina la conductivitat i propietats col·lectives. Fins i tot a química, permet entendre reaccions catalítiques basades en túnel d'electrons i protons, durant la fotosíntesi. D'aquesta manera, l'equació de Schrödinger no només explica el comportament de la matèria, sinó que impulsa tecnologies innovadores en múltiples àmbits.

Un dels seus experiments més famosos és el gat de Schrödinger, Erwin va inventar aquest experiment mental l'any 1935 per mostrar com d'estranyes i poc intuïtives són les regles de la mecànica quàntica quan s'apliquen a objectes grans, com un gos o un gat. La idea d'aquest físic era posar en evidència com seria d'absurd aplicar literalment la física quàntica al món quotidià.

Erwin volia que ens imaginéssim una caixa completament tancada on hi ha un gat. Un flascó de verí, un àtom radioactiu i un detector d'àtoms. L'experiment consisteix en: en una caixa com he dit hi ha dins un gat amb un flascó de verí i l'àtom radioactiu que hi ha dins té un 50% de possibilitats de desintegrar-se en una hora qualsevol. Si aquest es desintegra el verí s'allibera i el gat mor. Si no, el gat segueix viu.

Segons la física quàntica, l'àtom està en una superposició d'estats: s'ha desintegrat i no s'ha desintegrat al mateix temps, fins que algú ho observa. Com que el destí del gat depèn de l'àtom, el gat també està en una superposició d'estats: està viu i mort alhora, fins que obrim la caixa i mirem. Això és molt diferent del que passa al món quotidià, on les coses estan en un estat o en un altre, mai en els dos alhora.

A la vida real els objectes grans com gats, persones o pilotes no mostren aquesta superposició perquè estan formats per moltíssimes partícules i estan en contacte amb l'entorn (llum, aire…), cosa que fa que la superposició "col·lapsi" molt ràpid.

El que Schrödinger volia demostrar amb aquest experiment mental era que les regles quàntiques, que funcionen molt bé per a coses molt petites (àtoms, electrons…), semblen absurdes si les apliquem a objectes grans. No es tractava de defensar que els gats puguin estar vius i morts alhora, com sovint es malinterpreta, sinó de qüestionar la interpretació quàntica dominant i les seves implicacions. Aquesta paradoxa ens obliga a plantejar preguntes profundes com: "On està la frontera entre el món quàntic i el món real?" o "Què significa realment observar o mesurar alguna cosa?" (Schrödinger, 1935)[23].

[23] Schrödinger, E. (1935). The present situation in quantum mechanics. *Proceedings of the American Philosophical Society*

Per poder entendre millor aquest experiment ho farem amb coses quotidianes com una moneda (representa el gat), posem la moneda dins la caixa i la llancem, pot sortir cara o creu, però com la caixa està tancada mai sabrem que ha sortit. Segons la física quàntica i la superposició diria que la moneda està en “cara o creu alhora” fins que obrim la caixa i mirem[24] [25] [26]

2.3 Thomas Young

Thomas Young va néixer el 13 de juny de 1773 i va morir el 10 de Maig de 1829, va ser un dels científics més polifacètics i brillants del seu temps. Des de petit va destacar per la seva intel·ligència amb dos anys llegia i amb catorze dominava més de deu llengües. Es va formar en medicina i física a Londres, Edimburg i Göttingen. Va contribuir molt a la física amb el seu experiment de la doble escletxa on va demostrar la naturalesa ondulatòria de la llum. [27]

Imatge 6: Thomas Young
Extreta de: https://ca.wikipedia.org/wiki/Thomas_Young

Young va dur a terme l’experiment l'any 1801 és un dels experiments més famosos i fonamentals de la física quàntica, ja que com he dit demostra com la llum i la matèria poden comportar-se tant com a ones com com a partícules, i revela la naturalesa probabilística dels fenòmens quàntics.

S’utilitza una font que emet partícules individuals (com fotons o electrons) cap a una barrera que té dues escletxes molt estretes i properes. Darrere d’aquesta barrera es col·loca una pantalla de detecció que mostra on impacten les partícules que travessen les escletxes.

---

[24] María, Francisco. *Biografía y contribuciones de Edwin Schrödinger a la física cuántica* [en línia]. OK Diario, 21 de maig de 2025 [Consultat: 30 de Maig de 2025]. Disponible a: https://okdiario.com/ciencia/biografia-contribuciones-edwin-schrodinger-fisica-cuantica-14799161
[25] Clarín. *Explicación sencilla del gato de Schrödinger* [en línia]. Clarín, 20 de novembre de 2022 [Consultat: 27 d’abril de 2025]. Disponible a: https://www.clarin.com/viste/explicacion-sencilla-del-gato-de-schrodinger_0_RfEgmlSX0r.html
[26] Wikipedia. *Gat de Schrödinger* [en línia]. Wikipedia, data no disponible [Consultat: 27 d’abril de 2025]. Disponible a: https://es.wikipedia.org/wiki/Gato_de_Schr%C3%B6dinger
[27] Wikipedia. *Thomas Young* [en línia]. Wikipedia, data no disponible [Consultat: 27 d’abril de 2025]. Disponible a: https://es.wikipedia.org/wiki/Thomas_Young

Finalment, després de fer l'experiment, es poden observar diferents respostes. Si no s'observa per quina escletxa passa cada partícula, a la pantalla apareix un patró de franges clares i fosques, anomenat patró d'interferència. Aquest patró és característic de les ones, ja que es produeix quan les ones que passen per cada escletxa se superposen, reforçant-se en algunes zones (franges clares) i anul·lant-se en altres (franges fosques). Per altra banda, si s'observa o es detecta per quina escletxa passa cada partícula, el patró d'interferència desapareix i només es veuen dues franges alineades amb les escletxes, com si les partícules fossin petites boles que només poden passar per una escletxa o per l'altra, comportament propi de partícules clàssiques. Tal com explica Feynman, aquest experiment "conté el cor de la mecànica quàntica. Conté el sol misteri. I la base de tota la nostra incomprensió" (Feynman, Leighton, & Sands, 1965)[28].[29]

S'ha d'aclarir que a més a més hi ha una altra resposta més sorprenent, i és que, fins i tot si les partícules s'envien d'una en una, el patró d'interferència continua apareixent a mesura que s'acumulen molts impactes a la pantalla. Això suggereix que cada partícula no passa per una escletxa o per l'altra, sinó que, d'alguna manera, passa per totes dues alhora i el seu comportament està descrit per una ona de probabilitat. [30]

2.4 Entrellaçament quàntic

Al principi de la mecànica quàntica, tres grans ments: Albert Einstein, Boris Podolsky i Nathan Rosen, l'any 1935 van plantejar una situació estranya que sacsejaria els fonaments de la física. Amb el seu famós experiment mental EPR, van descobrir una propietat inquietant de la teoria quàntica: les partícules que havien interactuat, podien quedar misteriosament connectades, fins i tot quan

[28] Feynman, R. P., Leighton, R. B., & Sands, M. (1965). *The Feynman Lectures on Physics, Vol. 3: Quantum Mechanics*. Addison-Wesley.
[29] Pastor, Julen. *Física quàntica: L'experiment de la doble rendija* [en línia]. Dciencia, 28 de setembre de 2023 [Consultat: 27 d'abril de 2025]. Disponible a: https://www.dciencia.es/fisica-cuantica-el-experimento-de-la-doble-rendija/
[30] Resueltoos. *Efecto doble rendija* [en línia]. Resueltoos, 7 de març de 2024 [Consultat: 27 d'abril de 2025]. Disponible a: https://www.resueltoos.com/blog/fisica-y-quimica/efecto-doble-rendija

estaven molt separades. Einstein, que no estava còmode amb aquesta “acció fantasmagòrica a distància”, insistia que la teoria estava incompleta.

El pas important va arribar el 1964 amb John Stewart que va crear unes regles matemàtiques per posar a prova aquest fenomen. Bell va demostrar que si hi havia “variables amagades com deia Einstein, les partícules haurien de comportar-se d’una manera diferent.

La confirmació real va arribar anys després gràcies a Alain Aspect, John Clauser i Anton Zeilinger. Els seus experiments intel·ligents amb fotons entrelligats van demostrar clarament que les partícules quàntiques es comporten d’una manera que cap teoria normal pot explicar. Aquest èxit els va valdre el Premi Nobel de Física de 2022.

Però què és exactament aquest fenomen? Doncs és quan dues partícules quàntiques s’entrelliguen, els seus estats queden units per sempre. Podem separar-les anys llum de distància, però en mesurar una, l’altra “sap” immediatament què fer. No hi ha cap senyal que viatgi entre elles, simplement comparteixen una connexió que va més enllà de l’espai.

La raó d’aquest comportament estrany està en la naturalesa de la realitat quàntica. Les partícules entrelligades no són independents, sinó que formen un sistema únic. Quan mesurem una, tot el sistema canvia alhora, decidint l’estat de les dues partícules. Aquesta “no-localitat” quàntica ens diu que potser la separació entre coses no és tan clara com pensàvem.

El més sorprenent és que, tot i ser tan estrany, no va contra la teoria de la relativitat. No podem enviar missatges més ràpid que la llum amb això, però sí que ens mostra que l’univers està molt més connectat del que creiem. Des d’ordinadors quàntics fins a sistemes de seguretat impossibles de trencar, aquest fenomen està canviant la nostra tecnologia mentre seguim descobrint els misteris del món quàntic. Tal com va dir Einstein, es referia a l’entrellaçament quàntic com una “acció fantasmagòrica a distància” (*spooky action at a distance*), tot i que avui sabem que aquest efecte ha estat confirmat experimentalment i no viola cap llei de la relativitat (Einstein, Podolsky i Rosen, 1935)[31] [32].

3. És realment incompleta la mecànica quàntica?

L'experiment EPR (Einstein-Podolsky-Rosen) va plantejar una de les qüestions més fonamentals de la física moderna: descriu completament la realitat la mecànica quàntica? Per entendre la profunditat d'aquest debat, cal analitzar:

Einstein defensa amb vehemència que la teoria quàntica era incompleta, basant-se en tres pilars filosòfics essencials:

- **El realisme:** les propietats físiques existeixen independentment de qualsevol observació.
- **La localitat:** cap influència pot propagar-se més ràpid que la velocitat de la llum.
- **La casualitat:** els efectes sempre segueixen les seves causes en un ordre temporal ben definit.[33]

El fenomen de l'entrellaçament quàntic semblava violar aquests principis sagrats de la física clàssica en mostrar correlacions instantànies entre partícules, independentment de la seva separació espacial, el què Einstein anomena despectivament "acció fantasma a distància".

Enfront d'aquesta postura, Niels Bohr i l'escola de Copenhaguen defensaven la completesa de la teoria quàntica mitjançant tres conceptes revolucionaris:

- **La complementarietat:** certes propietats són inherentment complementàries i no poden mesurar-se simultàniament.
- **La contextualitat:** els resultats experimentals depenen crucialment del dispositiu de mesura complet.

[31] Einstein, A., Podolsky, B., & Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, *47 (10*), 777–780.
[32] Wikipedia. *Entrelazamiento cuántico* [en línia]. Wikipedia, data no disponible [Consultat: 2 de maig de 2025]. Disponible a: https://es.wikipedia.org/wiki/Entrelazamiento_cu%C3%A1ntico
[33] Paz, Juan Pablo (2007). *Einstein contra la mecánica cuántica: el azar, la ignorancia y nuestra ignorancia sobre el azar*. Buenos Aires: Departament de Física, FCEyN, UBA.

- **L'indeterminisme fonamental:** la probabilitat en mecànica quàntica no reflecteix ignorància sinó una característica intrínseca de la natura.

Els desenvolupaments teòrics posteriors, especialment el teorema de Bell el 1964 i la seva verificació experimental per Alain Aspect el 1982, han projectat llum sobre aquest debat, tot i que, sense cap motiu han generat noves i més profundes preguntes sobre la naturalesa de la realitat.[34]

3.1 Les variables ocultes: entre l'esperança i la refutació experimental

La recerca de variables ocultes ha estat un dels programes d'investigació més fascinants en els fonaments de la física quàntica, representant l'últim reducte del determinisme en el món microscòpic.

Les teories de variables ocultes locals, hereves directes del pensament einsteinià, mantenien que:

- Les partícules posseeixen propietats ben definides abans de qualsevol mesura.
- Les correlacions quàntiques podrien explicar-se mitjançant paràmetres ocults.
- Es preservava el principi de localitat relativista.

No obstant això, els experiments basats en les desigualtats de Bell han demostrat de manera concloent que cap teoria de variables ocultes locals pot reproduir totes les prediccions de la mecànica quàntica.

Com a alternativa, David Bohm va desenvolupar la seva teoria de variables ocultes no locals que, tot i ser compatible amb els experiments, introdueix complicacions conceptuals com:

- La necessitat d'una "ona pilot" que guiï les partícules
- La no-localitat explícita en les equacions fonamentals

[34] Greene, Jim (2024). *EPR paradox*. EBSCO Research Starters. [Consultat: 2 de maig de 2025]. Disponible a: https://www.ebsco.com/research-starters/physics/epr-paradox

- L'aparent violació de l'esperit (encara que no de la lletra) de la relativitat especial

Altres aproximacions, com les teories de col·lapse objectiu GRW o la proposta de Roger Penrose, busquen explicar la transició entre en món quàntic i el clàssic mitjançant mecanismes físics addicionals encara que cap ha aconseguit acceptació universal. [35] [36]

3.2 La de coherència quàntica: el pont entre dos mons

El misteri de per què no observem efectes quàntics en la vida quotidiana troba la seva explicació més convincent en el fenomen de la de coherència quàntica, que actua com un mecanisme ràpid i eficient de transició entre els dominis quàntic i clàssic.

Els processos físics responsables de la de coherència inclouen:

- La interacció amb fotons tèrmics omnipresents fins i tot en el buit
- Els camps electromagnètics fluctuants de l'entorn
- Les col·lisions moleculars en medis materials

Els temps característics de de coherència varien espectacularment segons l'escala:

- Per a sistemes atòmics poden persistir durant segons
- En sistemes mesoscòpics com molècules complexes només pico segons
- En objectes macroscòpics la de coherència és pràcticament instantània

Experiments pioners com els d'interferència amb ful·lerens el 1999 o més recentment amb molècules orgàniques complexes han explorat aquesta frontera difusa entre els mons quàntic i clàssic, revelant els límits de la nostra intuïció física.[37]

[35] García-Matos, Marta (2018). *El sentit quàntic IV: Per què?* Barcelona: Centre de Cultura Contemporània de Barcelona. [Consultat: 3 de maig de 2025]. Disponible a: https://lab.cccb.org/ca/el-sentit-quantic-iv-per-que/

[36] Wikipedia. *Teoría de variables ocultas* [en línia]. Wikipedia, data no disponible [Consultat: 3 de maig de 2025]. Disponible a: https://ca.wikipedia.org/wiki/Teoria_de_variables_ocultes

[37] Redacció. *Què és la decoherència quàntica i per què és clau per entendre el pas del món quàntic al clàssic* [en línia]. *Noticias de la Ciencia*, 16 de juny de 2025 [Consultat: 3 de maig de 2025]. Disponible a:

3.3 L'efecte túnel quàntic: quan l'impossible es torna quotidià

L'efecte túnel quàntic representa potser la manifestació més sorprenent i contraintuïtiva de la mecànica quàntica, on partícules travessen barreres energètiques que serien completament infranquejables segons la física clàssica.

La descripció matemàtica del fenomen en revela la naturalesa probabilística:

- La probabilitat de tunelització decau exponencialment amb l'amplada de la barrera.
- Depèn críticament de la massa de la partícula.
- Varia amb la diferència entre l'energia de la partícula i l'alçada de la barrera.

Aquest efecte aparentment exòtic té conseqüències pràctiques fonamentals:

- En les estrelles permet la fusió nuclear a temperatures insuficients clàssicament.
- En l'electrònica moderna és la base de memòries flaix i dispositius ultraràpids
- En biologia explica mutacions espontànies i l'eficiència de certs enzims.

Les implicacions filosòfiques de l'efecte túnel són profundes, qüestionant els nostres conceptes més bàsics de barrera física i trajectòria, mentre que les seves aplicacions tecnològiques continuen expandint-se en camps tan diversos com la medicina, la computació quàntica i la ciència de materials.

---

https://noticiasdelaciencia.com/art/54233/que-es-la-decoherencia-cuantica-y-por-que-es-clave-para-entender-el-paso-del-mundo-cuantico-al-clasico

4. Criptografia quàntica: El protocol BB84

La criptografia ha estat, des de fa segles, un pilar fonamental per garantir la seguretat de la informació. Amb l'avenç de la computació quàntica, molts sistemes criptogràfics clàssics, com el RSA, es poden veure amenaçats. En aquest context, la criptografia quàntica emergeix com una alternativa segura basada en les lleis de la física quàntica. Un dels protocols més coneguts i utilitzats és el BB84, desenvolupat l'any 1984 per Charles Bennett i Gilles Brassard, que «representa la base fonamental per a la distribució segura de claus quàntiques» (Bennett & Brassard, 1984)[38]. Aquest protocol no només va marcar el naixement de la criptografia quàntica, sinó que continua essent la pedra angular de molts sistemes actuals de distribució de claus quàntiques.

4.1 Context i fonaments de la criptografia quàntica

4.1.1 Limitacions de la criptografia clàssica

Els sistemes criptogràfics actuals, com RSA o ECC, es basen en la complexitat computacional de certs problemes matemàtics (factorització de nombres grans, logaritmes discrets, etc.) No obstant això, amb l'arribada dels ordinadors quàntics, aquests problemes poden ser resolts de manera eficient mitjançant l'algoritme de **Shor**, comprometen així la seguretat dels sistemes tradicionals.[39]

4.1.2 Principis de la criptografia quàntica

La criptografia quàntica aprofita fenòmens com:

- **Principi d'incertesa de Heisenberg:** és impossible mesurar l'estat d'un sistema quàntic sense alterar-lo.

[38] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175–179.

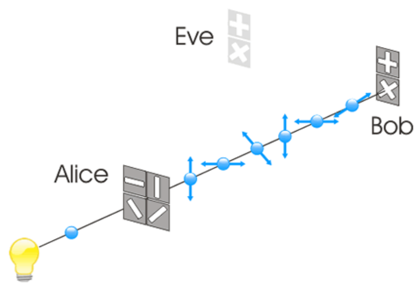
[39] Sectigo. *RSA vs DSA vs ECC Encryption* [en línia]. Sectigo, data no disponible [Consultat: 20 de juliol de 2025]. Disponible a: https://www.sectigo.com/es/recursos/rsa-vs-dsa-vs-ecc-encryption

- **Principi de no clonació:** no es pot copiar un estat quàntic desconegut de manera perfecta.

Gràcies a aquests principis, es poden detectar possibles intercepcions i garantir la confidencialitat de la informació transmesa.

4.2 El protocol BB84: visió general

El protocol BB84 és un mètode de distribució de claus quàntiques (Quantum Key Distribution, QKD). El seu objectiu és permetre que dos usuaris, generalment anomenats l'Alícia i el Bob, comparteixin una clau secreta que pugui ser utilitzada per encriptar missatges. L'Alícia seria "l'emissor", el que envia els missatges o la clau secreta, i el Bob seria "el receptor", que rep el missatge o la clau. A diferència de la criptografia tradicional, el BB84 no transmet informació útil per si sola, sinó que permet establir una clau simètrica segura, detectant qualsevol possible atac o intercepció durant el procés (Bennett y Brassard, 1984)[40].



Imatge 6: Thomas Young
Extreta de: https://ca.wikipedia.org/wiki/Thomas_Young

4.3 Funcionament del protocol BB84 pas a pas

4.3.1 Preparació de les bases i estats

El BB84 utilitza qubits (bits quàntics), que es poden preparar en diferents bases. Es defineixen dues bases ortogonals:

- **Base rectilínia (Z):**
  - $|0\rangle$ = polarització horitzontal
  - $|1\rangle$ = polarització vertical

[40] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175–179.

- **Base diagonal (X)**
    - |+⟩ = polarització a 45°
    - |-⟩ = polarització a 135°

Aquestes dues bases no són compatibles: si un qubit es mesura en una base diferent de la que va ser preparat, el resultat és aleatori.

Taula 1.

Bit	Base X (diagonal)
0	0⟩ (horitzontal)
1	1⟩ (vertical)

4.3.2 Etapes del protocol

- **Pas 1:** Generació aleatòria de bits i bases

  L'Alícia genera dues seqüències aleatòries:
    - Una de bits (0 o 1)
    - Una de bases (Z o X)

Per exemple:

Taula 2.

Posició	Bit	Base
1	0	Z
2	1	X
3	1	Z
4	0	X

- **Pas 2: Enviament de qubits:** L'Alícia codifica els bits segons la base triada i envia els qubits al Bob a través d'un canal quàntic

- **Pas 3: Elecció aleatòria de bases (Bob)**

  El Bob també tria bases aleatòriament per mesurar els qubits rebuts

Taula 3.

Posició	Base (Alícia)	Base (Bob)	Mesura correcta?
1	Z	Z	Sí
2	X	Z	No
3	Z	X	No
4	X	X	Sí

- **Pas 4: Comparació de bases:** Un cop finalitzada la transmissió, l'Alícia i el Bob comuniquen (a través d'un canal clàssic) quines bases van utilitzar, però no els valors dels bits. Només conserven les posicions on van utilitzar la mateixa base.

- **Pas 5: Extracció de la clau:** De les coincidències de bases, l'Alícia i el Bob conserven els bits corresponents. Aquesta nova seqüència és la clau secreta compartida.
- **Pas 6: Verificació de seguretat (opcional però recomanada):** Per detectar la presència d'un espia (generalment anomenat l'Eva), l'Alícia i el Bob comparen una part de la clau resultant. Si hi ha moltes discrepàncies, saben que algú ha intentat interceptar la comunicació i la clau és descartada.

4.4 Exemple pràctic del BB84

Simulació de la transmissió

- Seqüència de l’Alícia (bit + base):

Taula 4.

Posició	Bit	Base (Alícia)
1	0	Z
2	1	X
3	0	X
4	1	Z
5	1	X

Bases d’en Bob:

Taula 5.

Posició	Bases (Bob)
1	Z
2	X
3	Z
4	Z
5	X

Mesures correctes (bases coincideixen): posicions 1, 2, 4, 5

La clau resultant serà: bits de les posicions 1, 2, 4, 5

Clau: 0, 1, 1, 1

4.5 Atac d’intercepció i reenviament

El BB84 és segur gràcies al principi de no clonació i a l’impacte que una observació externa té sobre l’estat quàntic.

4.5.1 Atac d'intercepció i reenviament

Si l’Eva intercepta els qubits i intenta mesurar-los, ha de triar una base. Si encerta, pot reenviar el mateix qubit. Però si s’equivoca, altera l’estat i introdueix errors que l’Alícia i el Bob poden detectar quan comparin part de la clau.

Taula 6.

Posició	Base (Alícia)	Base (Eva)	Base (Bob)	Error introduït
1	Z	X	Z	Sí
2	X	X	X	No
3	Z	Z	Z	No

Com més qubits intercepta Eva, més errors es generen i més probable és que sigui detectada.[41] [42]

4.5.2 Taxa d’error i llindars

Normalment, si la taxa d’error detectada és superior a un cert llindar (sovint l'11% en sistemes reals), la clau es descarta. Això fa que el protocol sigui intrínsecament segur davant atacs de tercers.

[41] Martin Villafruela J.(2010). *Título del trabajo fin de grado*. Universidad de Valladolid. [Consultat: 20 de juliol de 2025]. Disponible a: https://uvadoc.uva.es/bitstream/handle/10324/60413/TFG-B.%202010.pdf?sequence=1
[42] Wikipedia. *Distribución cuántica de claves* [en línia]. Wikipedia, data no disponible [Consultat: 24 de juliol de 2025]. Disponible a: https://es.wikipedia.org/wiki/Distribuci%C3%B3n_cu%C3%A1ntica_de_claves

4.6 Implementacions reals i limitacions

4.6.1 Sistemes comercials

Des de la seva proposta el 1984, el protocol BB84 ha evolucionat des d'un concepte teòric fins a aplicacions pràctiques en entorns comercials i governamentals. Avui dia, diverses empreses i centres tecnològics han desenvolupat sistemes basats en BB84 capaços de generar i distribuir claus quàntiques a través de canals òptics, demostrant la viabilitat comercial i la seguretat d'aquest protocol en entorns reals (Gisin, Ribordy, Tittel, & Zbinden, 2002)[43].

Una de les empreses pioneres és *ID Quantique,* amb seu a Suïssa, que ofereix sistemes comercials de distribució de claus quàntiques (QKD). Els seus productes són utilitzats per governs, institucions bancàries i laboratoris per protegir comunicacions altament sensibles. Un exemple destacat és l'ús de la seva tecnologia en la protecció de dades diplomàtiques a través de la infraestructura de fibra òptica entre ambaixades.

"Toshiba" també ha fet grans avenços en la implementació del BB84. La seva divisió de recerca ha desenvolupat sistemes QKD capaços de funcionar en entorns urbans, fins i tot en fibres òptiques ja utilitzades per serveis d'internet. Toshiba ha desplegat una xarxa QKD a Londres per protegir dades financeres de clients institucionals.

Altres projectes com SECOQC (Secure Communication based on Quantum Cryptography), finançat per la Unió Europea, han demostrat que és possible construir una xarxa segura basada en QKD, combinant diverses tecnologies quàntiques i clàssiques per establir comunicació segura entre múltiples punts.

En l'àmbit asiàtic, destaca la Xin, que va posar en òrbita el primer satèl·lit dedicat a comunicacions quàntiques, Micius, amb el qual es va dur a terme una distribució de claus BB84 entre estacions terrestres separades per més de 1000 km, demostrant la viabilitat d'una infraestructura quàntica global.

---

[43] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, 74 (1), 145–195.

4.6.2 Limitacions pràctiques

Tot i el gran potencial del BB84, les implementacions actuals pateixen limitacions derivades de la tecnologia quàntica i dels canals de transmissió disponibles.

4.6.2.1 Distància de transmissió

Els senyals quàntics, en forma de fotons individuals, es transmeten habitualment per fibra òptica. A diferència de les dades clàssiques, no es poden amplificar mitjançant repetidors tradicionals, ja que qualsevol mesura del fotó altera el seu estat i invalida la clau. Aquesta limitació provoca que el senyal es degradi ràpidament a causa de l'atenuació del medi. Els sistemes comercials actuals poden arribar a 100-200 km, depenent de la qualitat de la fibra i dels detectors.

S'estan investigant solucions com els repetidors quàntics basats en entrellaçament i memòries quàntiques, però encara són tecnologies experimentals.

4.6.2.2 Eficiència de la clau

Una altra limitació inherent al BB84 és que només es conserven els bits en què l'Alícia i el Bob han escollit la mateixa base de mesura. Com que les bases es trien de forma aleatòria (Z o X), això implica que només un 50% de les transmissions es poden utilitzar per generar la clau secreta. Això redueix l'eficiència bruta del protocol.

La següent taula mostra un exemple simplificat:

Taula 7.

Fotó n.	Base Alícia	Polarització	Base bob	Mesura bob	Coincideix?
1	Z	0° (	0⟩)	X	aleatori
2	X	45° (	+⟩)	X	
3	Z	90° (	1⟩)	Z	
4	X	135° (	-⟩)	Z	aleatori

Només els fotons 2 i 3 s'utilitzarien per formar la clau.

4.6.2.3 Error tècnics i soroll

En el món real, els sistemes estan exposats a múltiples fonts de soroll i imperfeccions:

- Detectors amb eficiència limitada o falsos positius (detectors foscos).
- Pèrdues de fotons en la transmissió per fibra òptica.
- Errors d'alineació en els sistemes òptics
- Interferències ambientals (temperatura, vibracions…).

Per mitigar aquests problemes, s'inclouen processos com la correcció d'errors i l'amplificació de privadesa, però això redueix encara més la taxa de clau neta.

4.7 Variants i evolució del BB84

L'eficiència i la seguretat del BB84 han estat objecte d'intens estudi des de la seva proposta original. A continuació es presenten algunes de les variants més rellevants que han sorgit per millorar-lo i adaptar-lo a noves amenaces.

4.7.1 SARG04

El protocol SARG04 (2004) va ser desenvolupat per protegir-se millor contra l'atac d'intercepció i reenviament en sistemes amb fonts que emeten múltiples fotons. A diferència del BB84, no es basa només en la coincidència de bases, sinó també en el coneixement parcial que pot obtenir un possible atacant. Això el fa més robust en entorns amb fonts no ideals, encara que a costa d'una taxa de clau lleugerament inferior.

4.7.2 BBM92

El BBM92 és una versió del BB84 basada en l'entrellaçament quàntic en lloc de polaritzacions preparades. En aquest cas, l'Alícia i el Bob reben cadascun un qubit d'un parell entrellaçament i mesuren els seus estats en bases aleatòries. Gràcies a les correlacions perfectes que ofereix l'entrellaçament, poden construir una clau segura. És especialment útil en xarxes quàntiques distribuïdes o quan es treballa amb satèl·lits.

4.7.3 Decoy-state BB84

El Decoy-state BB84 afegeix polsos falsos o de prova (decoy pulses) a la transmissió. Això permet detectar i prevenir atacs de fotons múltiples, on un espia (Eva) podria detectar la presència de més d'un fotó i extreure informació. En introduir *decoys* amb intensitats diferents, l'Alícia i el Bob poden verificar la presència d'atacs mitjançant l'estadística de deteccions.

Aquestes variants han permès estendre el BB84 a escenaris més exigents, millorant la seguretat i la fiabilitat en entorns reals.

PART PRÀCTICA

La part pràctica d'aquest treball consisteix a implementar una simulació del protocol BB84 de criptografia quàntica, tal com s'ha descrit prèviament a la part teòrica. L'objectiu és observar, mitjançant programació en el llenguatge Python, el funcionament del protocol en un entorn controlat, tot reproduint els diferents passos que duen a terme els participants (Alícia, Bob i Eva). Aquesta simulació permet analitzar com es generen les claus quàntiques segures, com es detecta una possible intercepció per part d'un espia (Eva) i com es comporten els valors mesurats segons els principis de la mecànica quàntica. A través de Python, es poden visualitzar i quantificar paràmetres com la taxa d'errors, l'eficiència del protocol, el nombre de qubits útils i la influència de l'espionatge quàntic en la seguretat de la clau generada.

1. Què és Python

Python és un llenguatge de programació d'alt nivell, interpretat, de propòsit general i amb una sintaxi clara i llegible. Va ser creat per Guido van Rossum l'any 1991 amb la intenció de dissenyar un llenguatge que fos fàcil d'utilitzar, tant per a principiants com per a professionals, i que alhora fos prou potent per desenvolupar projectes complexos. Amb el pas dels anys, Python s'ha convertit en un dels llenguatges més populars i utilitzats arreu del món, gràcies a la seva simplicitat, versatilitat i una gran comunitat d'usuaris que contribueixen constantment amb biblioteques i eines.

Una de les característiques més destacades de Python és la seva sintaxi minimalista, que recorda molt l'estructura del llenguatge natural. Això el fa especialment atractiu per a aquelles persones que comencen a programar, ja que permet escriure codi de manera senzilla i intuïtiva. Per exemple, operacions bàsiques com condicions **(if),** bucles **(for, while)** i definició de funcions **(def)** es fan amb una estructura clara i fàcil d'entendre, evitant elements complicats com les clau **({})** o el punt i coma **(;)** que sí que apareixen en altres llenguatges com C o Java.

Python és també interpretat, cosa que significa que el codi es pot executar línia per línia sense necessitat de compilar-lo prèviament. Això fa que el procés de prova i error sigui molt més àgil i immediat. És ideal per a tasques com el prototipat ràpid, l'anàlisi de dades, la simulació, l'automatització de processos i el desenvolupament web.

En l'àmbit educatiu i científic, Python ha guanyat molta presència gràcies a la seva accessibilitat i al fet que s'utilitza tant en investigació acadèmica com en la indústria tecnològica. També és molt utilitzat en el camp de la física i la criptografia, ja que permet simular comportaments complexos de manera senzilla. És per aquest motiu que en aquest treball s'utilitzarà utilitzat Python per simular el protocol BB84 de criptografia quàntica, aprofitant la capacitat del llenguatge per generar aleatorietat estructurar processos lògics i mostrar resultats clars. [44]

1.1 Instruccions bàsiques de Python

Com s'ha esmentat abans, Python és un llenguatge de programació molt utilitzat tant per principiants com per professionals. Per començar a programar en Python, cal conèixer una sèrie de comandaments i estructures bàsiques que permeten fer operacions, controlar el flux del programa i manipular dades. A continuació, es presenten deu comandaments essencials que no només són útils per començar, sinó que també s'utilitzen constantment en projectes més avançats. Aquestes instruccions formen la base per entendre i construir qualsevol programa en Python:

1. **Input():** Permet demanar informació a l'usuari pel teclat

```
nom = input("Com et dius? ")
print("Hola,", nom)
```

Imatge 6. Captura de pantalla de Google Colab
Extreta de: Font pròpia

```
Com et dius? Alex
Hola, Alex
```

Imatge 7. Captura de pantalla de Google Colab
Extreta de: Font pròpia

[44] Wikipedia. *Python* [en línia]. Wikipedia, data no disponible [Consultat: 15 de juliol de 2025]. Disponible a: https://es.wikipedia.org/wiki/Python

2. **While:** Crea un bucle que es repeteix mentre una condició sigui certa:

```
x = 0
while x < 3:
    print("x és:", x)
    x += 1
```

Imatge 8. Captura de pantalla de Google Colab
Extreta de: Font pròpia

```
x és: 0
x és: 1
x és: 2
```

Imatge 9. Captura de pantalla de Google Colab
Extreta de: Font pròpia

3. **Len():** Retorna la longitud (nombre d'elements) d'una cadena, llista, etc.

```
paraula = "criptografia"
print("Lletres:", len(paraula))
```

Imatge 9. Captura de pantalla de Google Colab
Extreta de: Font pròpia

```
Lletres: 12
```

Imatge 10. Captura de pantalla de Google Colab
Extreta de: Font pròpia

4. **Range():** Genera una seqüència de nombres, sovint usada amb "*for*"

```
for i in range(1, 4):
    print("Número:", i)
```

Imatge 11. Captura de pantalla de Google Colab
Extreta de: Font pròpia

```
Número: 1
Número: 2
Número: 3
```

Imatge 12. Captura de pantalla de Google Colab
Extreta de: Font pròpia

5. **Append():** Afegeix un element al final d'una llista.

```
llista = [10, 20]
llista.append(30)
print("Llista:", llista)
```

Imatge 13. Captura de pantalla de Google Colab
Extreta de: Font pròpia

```
Llista: [10, 20, 30]
```

Imatge 14. Captura de pantalla de Google Colab
Extreta de: Font pròpia

6. **In:** Comprova si un valor està dins d'una llista, cadena, etc.

```
fruits = ["poma", "raïm", "kiwi"]
if "poma" in fruits:
    print("Hi ha poma!")
```

Imatge 15. Captura de pantalla de Google Colab
Extreta de: Font pròpia

```
Hi ha poma!
```

Imatge 16. Captura de pantalla de Google Colab
Extreta de: Font pròpia

7. **Elif:** Permet afegir condicions alternatives a un *"if"*

```python
x = 7
if x < 5:
    print("Petit")
elif x < 10:
    print("Mitjà")
else:
    print("Gran")
```

Imatge 17. Captura de pantalla de Google Colab
Extreta de: Font pròpia

```
Mitjà
```

Imatge 18. Captura de pantalla de Google Colab
Extreta de: Font pròpia

8. **Dict():** Crea estructures clau-valor, molt útils per organitzar informació.

```python
persona = dict(nom="Jordi", edat=25)
print("Nom:", persona["nom"])
print("Edat:", persona["edat"])
```

Imatge 19. Captura de pantalla de Google Colab
Extreta de: Font pròpia

```
Nom: Jordi
Edat: 25
```

Imatge 20. Captura de pantalla de Google Colab
Extreta de: Font pròpia

9. **Print():** Serveix per mostrar informació per pantalla

```python
print("Hola món")
```

Imatge 21. Captura de pantalla de Google Colab
Extreta de: Font pròpia

```
Hola món
```

Imatge 22. Captura de pantalla de Google Colab
Extreta de: Font pròpia

10. **Try/Except:** Controla errors i evita que el programa es bloquegi.

```python
try:
    resultat = 10 / 0
except ZeroDivisionError:
    print("No es pot dividir entre zero.")
```

Imatge 23. Captura de pantalla de Google Colab
Extreta de: Font pròpia

```
No es pot dividir entre zero.
```

Imatge 24. Captura de pantalla de Google Colab
Extreta de: Font pròpia

2. Simulació del protocol BB84 a Python.

Per començar a simular el protocol, primer ha estat necessari instal·lar Python a través de la Microsoft Store. Segons les recomanacions d'altres usuaris, aquesta aplicació funciona de manera òptima amb les versions compreses entre la 3.7 i la 3.11. Un cop instal·lat l'entorn, es pot començar a desenvolupar el codi del programa.

Aquest codi és una implementació pràctica del protocol BB84 de criptografia quàntica mitjançant Qiskit, una biblioteca de Python que permet crear i simular circuits quàntics. A diferència de les simulacions simplificades que es poder fer només amb operacions aleatòries, aquest codi fa servir circuits quàntics reals simulats per representar l'enviament, la mesura i fins i tot la intercepció d'informació quàntica. El seu objectiu és simular la transmissió de qubits entre dues persones (Alícia i Bob), amb la possibilitat que una tercera (Eva) intercepti part dels missatges.

Per començar, s'importen les biblioteques necessàries: "*random*" per generar valors aleatoris, i diversos mòduls de Qiskit com "*QuantumCircuit*", "*Aer*" i "*execute*", que serveixen per construir i executar els circuits quàntics.

protocol_bb84.py

Fitxer Edita Visualització

```
import random
from qiskit import QuantumCircuit, Aer, execute
```

Imatge 25. Captura de pantalla de Bloc de Notes
Extreta de: Font pròpia

Tot seguit, es defineix el nombre de qubits que es transmetran (en aquest cas, 100) i es generen tres llistes aleatòries: una amb els bits que l'Alícia vol enviar, una amb les bases (rectilínia o diagonal) que utilitzarà per codificar-los, i una altra amb les bases que farà servir en el Bob per mesurar-los. Els resultats de les mesures del Bob es guardaran en una llista buida.

```
n = 100  # nombre de qubits
alice_bits = [random.randint(0, 1) for _ in range(n)]
alice_bases = [random.randint(0, 1) for _ in range(n)]
bob_bases = [random.randint(0, 1) for _ in range(n)]
bob_results = []
```

Imatge 26. Captura de pantalla de Bloc de Notes
Extreta de: Font pròpia

El funcionament del sistema es basa en dues funcions fonamentals. La primera, “*encode_qubit* (bit, basis)”, prepara cada qubit segons el bit que l’Alícia vol transmetre i la base escollida. Si el bit és 1, s’aplica una porta X, que canvia l’estat $|0\rangle$ a $|1\rangle$. Si la base és la diagonal, es fa servir una porta Hadamard (H), que col·loca el qubit en superposició. Això reflecteix el comportament quàntic real: un mateix qubit pot estar en diferents estats segons com s’hagi preparat.

```
def encode_qubit(bit, basis):
    qc = QuantumCircuit(1, 1)
    if bit == 1:
        qc.x(0)
    if basis == 1:
        qc.h(0)
    return qc
```

Imatge 27. Captura de pantalla de Bloc de Notes
Extreta de: Font pròpia

La segona funció, “*eve_intercept*”, simula una situació en què l’Eva intercepta el qubit, el mesura en una base aleatòria, i després el torna a codificar abans d’enviar-lo al Bob. Aquest procés pot introduir errors, ja que si la base de l’Eva no coincideix amb la de l’Alícia, el qubit es veu alterat. Això és essencial per la seguretat del protocol BB84b: si hi ha un espia, es poden detectar discrepàncies en els bits mesurats pel Bob.

```
def eve_intercept(qc, eve_basis):
    if eve_basis == 1:
        qc.h(0)
    qc.measure(0, 0)
    result = execute(qc, Aer.get_backend('aer_simulator'), shots=1, memory=True).result()
    bit = int(result.get_memory()[0])
    return encode_qubit(bit, eve_basis)
```

Imatge 28. Captura de pantalla de Bloc de Notes
Extreta de: Font pròpia

El cor del programa és el bucle que recorre tots els qubits. Per cada qubit, primer es codifica segons les dades de l’Alícia. A continuació, amb una probabilitat del 50%, s’executa la funció d’intercepció de l’Eva, per simular un escenari realista on l’espia no intercepta tots els qubits. Finalment, el Bob aplica una transformació Hadamard si la seva base és la diagonal, mesura el qubit i guarda el resultat.

```
for i in range(n):
    qc = encode_qubit(alice_bits[i], alice_bases[i])

    if random.random() < 0.5:  # simulem intercepció d'Eve
        eve_basis = random.randint(0, 1)
        qc = eve_intercept(qc, eve_basis)

    if bob_bases[i] == 1:
        qc.h(0)
    qc.measure(0, 0)
    result = execute(qc, Aer.get_backend('aer_simulator'), shots=1, memory=True).result()
    bit = int(result.get_memory()[0])
    bob_results.append(bit)
```

Imatge 29. Captura de pantalla de Bloc de Notes
Extreta de: Font pròpia

Després d'acabar el programa, s'executa a la terminal de l'ordinador posant *"python, i el nom del fitxer".* I surt el següent:

```
Microsoft Windows [Versión 10.0.22631.5335]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\EricGarciaDoñate> cd Documents

C:\Users\EricGarciaDoñate\Documents> python protocol_bb84.py
Traceback (most recent call last):
  File "C:\Users\EricGarciaDoñate\Documents\protocol_bb84.py", line 2, in <module>
    from qiskit import QuantumCircuit, Aer, execute
ImportError: cannot import name 'Aer' from 'qiskit' (C:\Users\EricGarciaDoñate\AppData\Local\Packages\PythonSoftwareFoundation.Python.3.11_qbz5n2kfr
a8p0\LocalCache\local-packages\Python311\site-packages\qiskit\__init__.py)

C:\Users\EricGarciaDoñate\Documents>
```

Imatge 30. Captura de pantalla de la Terminal del ordinador
Extreta de: Font pròpia

Aquest error indica que a l'ordinador falta instal·lar la biblioteca **Qiskit**. Per fer-ho, executem a la terminal la comanda següent:

pip install qiskit[all]

Aquesta instrucció instal·la tot el paquet de recursos de Qiskit (*qiskit, qiskit-aer, qiskit-terra, qiskit-ibmq-provider*, així com les extensions visuals i funcionals).

Tot i això, en tornar a executar el programa apareix el mateix error. Per resoldre-ho, forcem la instal·lació i provem de nou, però el problema persisteix. Finalment, actualitzem totes les instal·lacions i apareix el missatge següent:

```
ERROR: Could not install packages due to an OSError: [Errno 2] No such file or directory: 'C:\\Users\\EricGarciaDoñate\\AppData\\Local\\Packages\\Py
thonSoftwareFoundation.Python.3.11_qbz5n2kfra8p0\\LocalCache\\local-packages\\Python311\\site-packages\\pkg_resources\\tests\\data\\my-test-package_
unpacked-egg\\my_test_package-1.0-py3.7.egg\\EGG-INFO\\dependency_links.txt'
HINT: This error might have occurred since this system does not have Windows Long Path support enabled. You can find information on how to enable th
is at https://pip.pypa.io/warnings/enable-long-paths
```

Imatge 31. Captura de pantalla de la Terminal del ordinador
Extreta de: Font pròpia

Aquest error indica que Python no admet més de 260 caràcters en les rutes d'arxius. Això passa perquè la versió de Python instal·lada des de la Microsoft Store és menys funcional que la que es pot descarregar directament des de la pàgina oficial de Python.

Per resoldre tots aquests problemes, es va decidir instal·lar l'aplicació des de la pàgina oficial de "python.com". Tot i així, van sorgir noves dificultats i finalment es va optar per utilitzar un ordinador personal per a facilitar el procés d'instal·lació.

Es va tornar a instal·lar Python i tots els paquets de Qiskit a l'ordinador personal, però continuaven apareixent els mateixos errors, com ara que Aer no es podia importar des de Qiskit.

```
C:\Users\[redacted]\Downloads> python test_qiskit_aer.py
Traceback (most recent call last):
  File "C:\Users\[redacted]\Downloads\test_qiskit_aer.py", line 10, in <module>
    from qiskit import Aer
ImportError: cannot import name 'Aer' from 'qiskit' (C:\Users\[redacted]\AppData\Local\Programs\Python\Python311\Lib\site-packages\qiskit\__init__.py)

C:\Users\[redacted]\Downloads>
```

Imatge 32. Captura de pantalla de la Terminal del ordinador
Extreta de: Font pròpia

Aquesta situació va fer replantejar la possibilitat que Python no funcionés correctament, tot i haver instal·lat tots els recursos necessaris per executar el programa. Després d'investigar, es va decidir provar el codi en un emulador capaç d'executar Python, concretament Google Colab. Tot i així, l'error persistia. Fins i tot es va fer una prova amb la resta d'elements per comprovar si realment eren ells els que provocaven l'errada.

```
from qiskit import QuantumCircuit, Aer, execute

print("Qiskit funciona correctament!")
```

```
---------------------------------------------------------------------------
ImportError                               Traceback (most recent call last)
/tmp/ipython-input-3-2471568745.py in <cell line: 0>()
----> 1 from qiskit import QuantumCircuit, Aer, execute
      2
      3 print("Qiskit funciona correctament!")

ImportError: cannot import name 'Aer' from 'qiskit' (/usr/local/lib/python3.11/dist-
packages/qiskit/__init__.py)

---------------------------------------------------------------------------
NOTE: If your import is failing due to a missing package, you can
manually install dependencies using either !pip or !apt.

To view examples of installing some common dependencies, click the
"Open Examples" button below.
---------------------------------------------------------------------------
```

Imatge 33. Captura de pantalla de Google Colab
Extreta de: Font pròpia

Finalment, es va optar per desenvolupar un altre programa, ja que resultava impossible corregir l'error que apareixia de manera constant. Aquest nou programa era més senzill de crear, ja que no requeria cap comandament complicat i tots eren força assequibles.

El codi es divideix en cinc parts principals. La primera correspon als *imports* i a la configuració inicial. En aquest apartat es defineixen els paràmetres bàsics: *n* controla la longitud de la seqüència de qubits que s'enviarà en una sessió del protocol, mentre que *"eve_prob"* determina la probabilitat que cada qubit sigui interceptat per l'Eva. Per exemple, si "*eve_prob*" = *0.5*, això significa que, de mitjana, l'Eva interceptarà la meitat dels qubits. Finalment, el comptador *mesuraments* s'inicia a zero i augmenta cada vegada que se simula una mesura quàntica, cosa que permet tenir un registre quantitatiu de l'activitat del protocol.

```
import random
import math

class BB84Simple:
    def __init__(self, n=50, eve_prob=0.0):
        self.n = n
        self.eve_prob = eve_prob
        self.measurements = 0
```

Imatge 34. Captura de pantalla de Bloc de Notes
Extreta de: Font pròpia

La segona part seria el *nucli quàntic* del programa. Aquesta funció és el cor físic del simulador. El que fa és reproduir el comportament d'un qubit quan és mesurat. Si la base de preparació "*prep_base*" i la base de mesura "*meas_base*" coincideixen, el resultat és determinista i retorna exactament el bit que l'Alícia havia preparat. Si les bases no coincideixen, la mesura esdevé completament aleatòria: el qubit entra en un estat de superposició respecte a la nova base i col·lapsa a un valor 0 o 1 amb probabilitat del 50% cadascun.

```
def measure_quantum(self, bit, prep_base, meas_base):
    self.measurements += 1
    if prep_base == meas_base:
        return bit
    else:
        return random.randint(0, 1)
```

Imatge 35. Captura de pantalla de Bloc de Notes
Extreta de: Font pròpia

En el context del BB84 utilitzem dues bases:

- Base rectilínia (0):

- Bit 0 → estat |0⟩
- Bit 1 →estat |1⟩

- Base diagonal (1)
    - Bit 0 → estat |+⟩
    - Bit 1 → estat |-⟩

Com a exemple clàssic s'exposa el següent: si l'Alícia prepara el qubit |+⟩ (bit 0 en base diagonal) i el Bob mesura en base rectilínia, el resultat serà 0 o 1 amb igual probabilitat, i per tant el Bob no pot recuperar amb certesa la informació original. Aquest comportament és el que permet que BB84 detecti un espionatge: quan es mesura en bases diferents, la informació original es perd i això introdueix errors que es poden comptar.

L'atac per part de l'Eva seria la tercera part. Aquesta funció implementa l'atac d'intercepció i reenviament "*eve_attack*". L'Eva, per cada qubit que decideix interceptar, tria una base aleatòria "*eve_base*" i el mesura utilitzant la mateixa funció "*measure_quantum*". A continuació, en lloc de reenviar el qubit original, envia al Bob un nou qubit preparat amb el resultat obtingut i en la base que ella ha utilitzat.

```
def eve_attack(self, bit, alice_base):
    eve_base = random.randint(0, 1)
    eve_result = self.measure_quantum(bit, alice_base, eve_base)
    return eve_result, eve_base
```

Imatge 36. Captura de pantalla de Bloc de Notes
Extreta de: Font pròpia

Si l'Eva encerta la base original de l'Alícia, no introdueix cap error. Però si tria la base equivocada, el resultat és aleatori i el qubit que reenvia al Bob pot estar alterat respecte de l'original. Això fa que, en mitjana, si intercepta tots els qubits, la taxa d'errors introduïda sigui aproximadament del 25%. Per exemple, si l'Alícia envia l'estat |0⟩ (bit 0, base rectilínia) i l'Eva mesura en base diagonal, obtindrà un 0 o un 1 aleatòriament; si obté un 1, reenviarà |-⟩ i el Bob, en mesurar en base rectilínia, tindrà un 50% de probabilitat de llegir un valor incorrecte.

```
        alice_bits = [random.randint(0, 1) for _ in range(self.n)]
        alice_bases = [random.randint(0, 1) for _ in range(self.n)]
```

Imatge 37. Captura de pantalla de Bloc de Notes
Extreta de: Font pròpia

A la quarta part seria **l'execució principal**, primer es prepara el que fa l'Alícia. Aquesta genera una seqüència de "n" bits i "n" bases aleatòries, codificant cada bit en l'estat quàntic corresponent. Aquesta aleatorietat és clau per a la seguretat del protocol, ja que un espia no pot predir amb antelació la combinació de bits i bases.
Seguidament, es busca la possible intercepció, se simula l'enviament dels qubits.

```
transmitted_bits = []
transmitted_bases = []
eve_count = 0

for i in range(self.n):
    bit, base = alice_bits[i], alice_bases[i]
```

Imatge 38. Captura de pantalla de Bloc de Notes
Extreta de: Font pròpia

Per cada un, decideix de forma probabilística si l'Eva l'intercepta o no, basant-se en "*eve_prob*". Si hi ha intercepció, el qubit i la base poden canviar segons el resultat de "*eve_attack*".

```
    if random.random() < self.eve_prob:
        bit, base = self.eve_attack(bit, base)
        eve_count += 1

    transmitted_bits.append(bit)
    transmitted_bases.append(base)
```

Imatge 39. Captura de pantalla de Bloc de Notes
Extreta de: Font pròpia

Quan el Bob rep els qubits, genera també la seva pròpia seqüència de bases de mesura de manera completament aleatòria. Tot seguit, mesura cada qubit que li arriba utilitzant la funció "*measure_quantum*". Si les seves bases coincideixen amb les de l'Alícia, obté exactament el mateix bit; si no coincideixen, el resultat és aleatori, fet que introdueix soroll al sistema.

```
bob_bases = [random.randint(0, 1) for _ in range(self.n)]
bob_results = []

for i in range(self.n):
    result = self.measure_quantum(transmitted_bits[i], transmitted_bases[i], bob_bases[i])
    bob_results.append(result)
```

Imatge 40. Captura de pantalla de Bloc de Notes
Extreta de: Font pròpia

Un cop el Bob ha realitzat totes les mesures, l'Alícia i el Bob comparen públicament les bases que han utilitzat, però sense revelar els valors dels bits. Gràcies a aquesta comparació, poden descartar totes aquelles posicions en què les seves bases no coincideixen, ja que en aquests casos

```
sifted_alice = []
sifted_bob = []

for i in range(self.n):
    if alice_bases[i] == bob_bases[i]:
        sifted_alice.append(alice_bits[i])
        sifted_bob.append(bob_results[i])
```

Imatge 41. Captura de pantalla de Bloc de Notes
Extreta de: Font pròpia

el resultat del Bob no és fiable. Aquest pas s’anomena filtratge, i normalment redueix la seqüència original a la meitat.

Finalment, amb les seqüències filtrades a les mans, l’Alícia i el Bob poden calcular la taxa d’errors comparant bit a bit. Si el percentatge d’errors és molt baix (pràcticament zero en absència de l’Eva), poden confiar que la clau és segura. En canvi, si la taxa d’errors és alta (fins a prop del 25% quan l’Eva ho intercepta tot), això és una evidència d’espionatge.

```
errors = sum(a != b for a, b in zip(sifted_alice, sifted_bob))
error_rate = errors / len(sifted_alice) * 100
efficiency = len(sifted_alice) / self.n * 100

print(f"Eficiència: {efficiency:.0f}% ({len(sifted_alice)}/{self.n} bits)")
print(f"Errors: {errors}, Taxa: {error_rate:.1f}%")
print(f"Eva interceptà: {eve_count} qubits")

if error_rate <= 11:
    print("SEGUR - Clau utilitzable")
else:
    print("INSEGUR - Possible espia detectat")
```

Imatge 42. Captura de pantalla de Bloc de Notes
Extreta de: Font pròpia

El llindar habitual se situa al voltant de l’11%: per sota, la clau s’accepta; per sobre, el protocol s'avorta.

Finalment, l’última part serien les funcions de demostracions. La funció “demo” comença imprimint un missatge que indica que s’indica una demostració i tot seguit executa tres simulacions consecutives. En cadascuna d’aquestes execucions, el nombre de qubits i la probabilitat d’intercepció de l’Eva són triats de manera aleatòria.

```
def demo():
    print("Demo BB84")

    for i in range(3):
        n_qubits = random.randint(30, 200)
        eve_prob = random.uniform(0.0, 0.9)

        print(f"Execució {i+1}: {n_qubits} qubits, Eva {eve_prob*100:.1f}%")
        bb84 = BB84Simple(n=n_qubits, eve_prob=eve_prob)
        bb84.run()
```

Imatge 43. Captura de pantalla de Bloc de Notes
Extreta de: Font pròpia

Això permet observar com es comporta el protocol sota diferents condicions i com canvia el resultat segons si l’Eva espia més o menys.

A la pràctica, això significa que en una execució es poden simular per exemple 45 qubits amb un 10% de probabilitat d’intercepció, en una altra 120 qubits amb un

60% de probabilitat i en una tercera 180 qubits amb un 5%. Aquestes variacions mostren clarament que com més gran és la probabilitat d'espionatge, més errors es detecten en la clau final, i que per sota del llindar de l'11% encara es pot considerar segura mentre que per sobre s'ha d'abandonar.

```
def principio_cuantico():
    print("Principi quàntic")
    print("Preparar |+⟩ i mesurar en base rectilínia:")

    bb84 = BB84Simple()
    resultados = []

    for _ in range(1000):
        resultado = bb84.measure_quantum(bit=0, prep_base=1, meas_base=0)
        resultados.append(resultado)

    ceros = resultados.count(0)
    unos = resultados.count(1)

    print(f"Resultats: {ceros} zeros, {unos} uns")
    print(f"Probabilitats: {ceros/10:.1f}% zeros, {unos/10:.1f}% uns")
    print("Incertesa quàntica confirmada")
    print()
```

Imatge 44. Captura de pantalla de Bloc de Notes
Extreta de: Font pròpia

La segona funció és "principi quàntic", té com a objectiu demostrar un dels fonaments de la mecànica quàntica en què es basa BB84: el fet que si un estat es aleatori. La funció prepara repetidament l'estat |+⟩, que correspon al bit 0 en base diagonal, i la mesura en base rectilínia. Aquest procés es repeteix mil vegades i es compten els resultats.

En executar aquesta funció, els resultats mostren que aproximadament la meitat de les vegades es mesura un 0 i l'altra meitat un 1, és a dir, uns 500 zeros i un 500 uns, amb petites variacions degudes a l'atzar. Això confirma que no és possible predir el resultat de la mesura quan les bases són diferents i il·lustra de manera pràctica el principi d'incertesa quàntica.

Finalment, el bloc principal del programa combina ambdues funcions. Primer crida "demo" per executar tres simulacions generals i després mostra un exemple individual més concret en què es genera un nombre de qubits i una probabilitat d'intercepció de l'Eva també de manera aleatòria, però dins uns marges més acotats.

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

    print("Exemple individual:")
    qubits = random.randint(40, 150)
    eva = random.uniform(0.05, 0.6)
    print(f"Qubits: {qubits}, Eva: {eva*100:.1f}%")

    bb84 = BB84Simple(n=qubits, eve_prob=eva)
    bb84.run()
```

Imatge 40. Captura de pantalla de Bloc de Notes
Extreta de: Font pròpia

Amb aquest bloc, el programa garanteix que cada execució sigui diferent, ja que en cada ocasió el nombre de qubits i la intensitat de l'espionatge de l'Eva varien. Per exemple, podria executar-se amb 100 qubits i un 20% de probabilitat d'intercepció o bé amb 75 qubits i un 50% de probabilitat, cosa que permet comprovar com l'augment d'intercepcions genera una taxa d'errors més alta i condueix a la detecció de l'espia.

Havent explicat ja la teoria del codi del programa fem funcionar el programa a Google Colab, que com ja s'ha esmentat, és un emulador de python a la xarxa. I la resposta que ens dona seria la següent:

```
Execució 1: 166 qubits, Eva 17.5%
BB84 - 166 qubits, Eva: 18%
Eficiència: 45% (74/166 bits)
Errors: 7, Taxa: 9.5%
Eva interceptà: 36 qubits
SEGUR - Clau utilitzable
Alícia: [0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1]
Bob:    [0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1]
```

Imatge 41. Captura de pantalla de Google Colab
Extreta de: Font pròpia

```
Exemple individual:
Qubits: 53, Eva: 26.8%
BB84 - 53 qubits, Eva: 27%
Eficiència: 51% (27/53 bits)
Errors: 3, Taxa: 11.1%
Eva interceptà: 16 qubits
INSEGUR - Possible espia detectat
Alícia: [1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1]
Bob:    [1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1]
```

Imatge 42. Captura de pantalla de Google Colab
Extreta de: Font pròpia

El programa genera dos tipus de resultats diferenciats: les execucions i l'exemple individual. Tot i que ambdós responen al mateix objectiu, responen i presenten algunes diferències.

Les execucions corresponen a la funció "demo()", que realitza tres simulacions automàtiques consecutives. En cadascuna d'elles, el nombre de qubits transmesos es tria aleatòriament dins d'un interval de 30 a 200, i la probabilitat d'intercepció de l'Eva també es genera de manera aleatòria entre el 0% i el 90%. Aquest conjunt d’execucions té com a finalitat mostrar diferents escenaris possibles, amb baixa, mitjana o alta presència d’un espia, i permet observar de quina manera varia la taxa d’errors i la seguretat de la clau compartida segons la intensitat de l’atac.

En canvi, l’exemple individual es calcula fora de la funció “demo()” i constitueix una simulació addicional i independent. En aquest cas, els valors també es generen de manera aleatòria, però dins d’un interval diferent: entre 40 i 150 qubits i amb una probabilitat d’intercepció d’entre el 5% i el 60%. L’objectiu d’aquest apartat no és mostrar una sèrie de casos sinó il·lustrar un escenari concret i analitzar-lo amb més detall, tot evidenciant que el protocol manté el seu comportament característic en qualsevol configuració

En l'execució, es transmeten un total de 166 qubits, dels quals l’Eva en va interceptar aproximadament un 18%. Després del procés de filtratge, l’Alícia i el Bob conserven 74 bits vàlids, el que representa una eficiència del 45%. L’anàlisi mostra que només hi ha 7 discrepàncies entre les claus dels dos usuaris, cosa que correspon a una taxa d’errors del 9,5%. Aquesta xifra es manté per sota del llindar de l'11%, que és el valor crític establert en el protocol per determinar si una clau és segura o bé ha estat compromesa. En conseqüència, la clau generada en aquesta execució es en la seva totalitat, amb diferències anecdòtiques que es poden eliminar mitjançant tècniques de correcció d’errors i amplificació de privacitat.

En l’exemple individual es van transmetre 53 qubits amb una intercepció intermèdia d’un 27% per part de l’Eva. El procés de filtratge redueix la clau a 27 bits útils, amb una eficiència del 51%. En aquest cas es detecten 3 errors, que corresponen a una taxa de l’11,1%. Malgrat que aquesta taxa és molt propera al límit establert, el fet de superar-lo encara que sigui lleugerament comporta que la clau es classifiqui com a insegura, ja que el protocol BB84 està dissenyat per prioritzar la seguretat per damunt de l’eficiència. Així, la mínima sospita d’una intercepció obliga l’Alícia i el Bob a descartar la clau i a reiniciar el procés de transmissió.

Cal destacar que els resultats obtinguts en la simulació del protocol no són sempre els mateixos, si no que varien cada vegada que es torna a executar el programa. Això és conseqüència directa de la mateixa naturalesa aleatòria del procés quàntic.

```
Execució 2: 64 qubits, Eva 80.2%
BB84 - 64 qubits, Eva: 80%
Eficiència: 59% (38/64 bits)
Errors: 9, Taxa: 23.7%
Eva interceptà: 52 qubits
INSEGUR - Possible espia detectat
Alícia: [1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0]
Bob:    [1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0]
```

Imatge 43. Captura de pantalla de Google Colab
Extreta de: Font pròpia

```
Execució 3: 196 qubits, Eva 84.2%
BB84 - 196 qubits, Eva: 84%
Eficiència: 45% (88/196 bits)
Errors: 17, Taxa: 19.3%
Eva interceptà: 156 qubits
INSEGUR - Possible espia detectat
Alícia: [0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1]
Bob:    [0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1]
```

Imatge 44. Captura de pantalla de Google Colab
Extreta de: Font pròpia

3. Anàlisi

S'han realitzat diverses execucions del protocol per avaluar el seu comportament davant atacs d'intercepció. Seguidament, trobareu 4 taules d'anàlisis, la primera les dades de les execucions, la segona una anàlisi estadística, una comparació per nivell d'intercepció i l'eficiència del protocol.

3.1. Taula 1: Dades de les execucions

Taula 8.

Execució	**Qubits**	**Eva (%)**	**Eficiència**	**Errors**	**Taxa error (%)**	**Intercepció Eva**	**Resultat**
1	166	17,5%	45% (74/166)	7	9,5 %	36 qubits	Segur
2	64	80,2%	59%	9	23,7%	52 qubits	Insegur

			(38/64)				
3	196	84.2	45% (88/196)	17	19.3	156 qubits	Insegur
4	53	26.8	51% (27/53)	3	11.1	16 qubits	Límit

Aquesta és una taula resum de les quatre execucions tal qual surten a les captures de pantalla anteriorment. Mostra cada sessió individual de distribució de claus quàntiques.

3.2. Taula 2: Anàlisi Estadístic

Taula 9.

Mètrica	Mínim	Màxim	Mitjana
Qubits generats	53	196	119.75
Eva (%)	17.5	84.2	52.2
Eficiència (%)	45	59	50
Taxa d'error (%)	9.5	23.7	15.9
Qubits interceptats	16	156	65

Es resumeixen les execucions amb mínim, màxim i mitjana de les mètriques. La mitjana de qubits generats és 119.75 amb gran variabilitat per simular condicions reals. El mínim seria el valor més petit observat en totes les execucions. El màxim el valor més gran observat i la mitjana seria el valor mitjà, indicant el comportament típic del sistema.

3.3. Taula 3: Comparació per nivell d'intercepció

Taula 10.

Nivell Eva	Rang (%)	Taxa error mitjana	Detecció	Risc
BAIX	<30%	10,3%	No	Baix

MITJÀ	30-50%	-	-	-
ALT	50-85%	21,5%	Si	Alt
EXTREM	>85%	19,3%	Si	Molt alt

Les sessions es classifiquen segons la intensitat de l'atac d'Eva: baix, mitjà, alt i extrem. S'observa que més intercepció genera més errors. Els errors baixos poden passar desapercebuts, mentre que els alts permeten detectar l'espia. El rang seria la diferència entre màxim i mínim, que reflecteix la variabilitat de les dades.

3.4. Taula 4: Eficiència del protocol

Taula 11.

Paràmetre	Valor	Interpretació
Eficiència teòrica	± 50%	Correcte (sifting elimina ± 50%)
Eficiència observada	50%	Coincideix amb teoria
Llindar de seguretat	11%	Límit màxim d'error acceptable
Sessions segures	25%	75% compromeses per Eva alta

L'eficiència observada coincideix amb la teòrica (50%), demostrant que el protocol BB84 manté correctament la proporció de bits útils. Tot i això, només una de quatre sessions aconsegueix clau segura quan Eva actua intensament, indicant que la protecció depèn directament del nivell d'intervenció.

Conclusions

Durant el desenvolupament d'aquesta investigació, es va construir un pont sòlid que connecta els fonaments de la mecànica quàntica amb la criptografia pràctica, concretament amb l'ús del protocol BB84. Les troballes obtingudes ofereixen una forta evidència sobre la possibilitat d'identificar intromissions en la comunicació, gràcies a les característiques essencials dels sistemes quàntics, la qual cosa confirma la idea principal de l'estudi. La simulació per ordinador va resultar ser una eina sorprenentment útil per entendre i verificar el comportament del protocol, tot i executar-se en un context clàssic que imita esdeveniments quàntics.

La investigació realitzada obre un ventall de possibilitats per a futures línies d'estudi que podrien expandir significativament l'abast i la profunditat del nostre coneixement en criptografia quàntica simulada. Una de les direccions més prometedores seria la implementació amb biblioteques especialitzades en computació quàntica, com Qiskit o QuTiP, que permetria superar les limitacions tècniques actuals. Aquest pas endavant facilitaria la simulació d'autèntics estats quàntics en lloc de la simple emulació del seu comportament.

No obstant això, la investigació va mostrar limitacions considerables que cal tenir en compte. La impossibilitat d'utilitzar biblioteques especialitzades de computació quàntica, a causa de problemes tècnics recurrents, va obligar a emprar una implementació simplificada que, tot i capturar l'essència del protocol, no opera amb estats quàntics reals. Aquesta limitació va impedir l'exploració de fenòmens complexos com en les imperfeccions en els detectors, aspecte crucial en les implementacions reals de criptografia quàntica.

Els reptes pendents identificats en aquesta investigació obren múltiples línies de treball futur. La superació de les barreres tècniques per incorporar biblioteques especialitzades com Qiskit o QuTiP permetria realitzar simulacions més precises i realistes.

Una de les futures investigacions podria expandir-se cap a la simulació de variants més sofisticades del protocol BB84, com el protocol SARG04 que ofereix majors garanties de seguretat, implementacions basades en entrellaçament quàntic seguint l'esquema BBM92, protocols amb estats senyal que millorin la seguretat i variants adaptades a xarxes quàntiques complexes.

La hipòtesi que es va presentar al principi del treball és la següent: si es duu a terme una simulació del protocol BB84 utilitzant un entorn de programació com Python, amb el suport de biblioteques especialitzades en computació quàntica com QuTiP o Qiskit, és possible detectar qualsevol intent d'intercepció en la transmissió de claus quàntiques. Després de la recerca realitzada la hipòtesi és validada parcialment, donat que el programa a Python sí que ha pogut detectar qualsevol intent d'intercepció en la transmissió de claus quàntiques, però donat a les limitacions tècniques que s'han comentat al treball no han pogut validar-se amb la implementació de biblioteques quàntiques.

A més a més, ha complert satisfactòriament la major part dels objectius inicials, suposant una aportació rellevant a la comprensió i implementació de protocols de criptografia quàntica mitjançant simulacions computacionals.

Es va dur a terme una anàlisi exhaustiva dels orígens de la física quàntica i un estudi profund del protocol BB84, establint una sòlida base teòrica. Tot i les dificultats amb biblioteques especialitzades com Qiskit, es va desenvolupar amb èxit un simulador funcional utilitzant Python reproduint les fases del protocol.

Els resultats més rellevants van ser la validació experimental dels principis de seguretat: mitjançant simulacions d'atacs es va demostrar quantitativament com la presència d'un espia (Eva) es tradueix en un augment significatiu d'errors a la clau final. L'anàlisi comparativa va confirmar la capacitat del protocol per detectar intents d'espionatge, amb taxes d'error que superaven el llindar de seguretat de l'11% quan la intercepció era elevada.

El treball també va permetre avaluar críticament els límits i potencialitats del BB84, identificant tant els seus punts forts (detecció fiable), com les seves limitacions (eficiència del 50%). Aquesta investigació estableix les bases per a futurs desenvolupaments en l’aplicació pràctica d’aquestes tecnologies en sistemes reals de comunicació segura, demostrant la viabilitat de validar principis de criptografia quàntica mitjançant simulacions computacionals.

Agraïments

En primer lloc, voldria agrair a la Maite Luque, la meva primera tutora del Treball de Recerca, per haver-me iniciat en el món de la recerca i haver-me guiat en el procés, i, en segon lloc, a la Dori Cañal la meva segona tutora del Treball de recerca, perquè em va agafar en un moment crític del treball i ha sabut guiar-me en tot moment i donar-me idees per poder seguir cap endavant el treball.

En tercer lloc, voldria agrair a la Leire Aguilar Tarragón, estudiant de la carrera de matemàtiques a la Universitat de València, per ajudar-me en tot moment amb el programa de Python.

I per últim, però no menys important, als meus amics i familiars que m'han donat suport moral tots aquests mesos tan intensos, per ajudar-me a buscar solucions sempre que m'enfrontava a qualsevol problema i estar sempre per mi quan necessitava qualsevol cosa del treball.

Bibliografia i Webgrafia

1. **Acadèmia EITCA.** *Quin és el concepte de superposició en mecànica quàntica i com es relaciona amb el comportament dels qubits en un sistema de N-qubits?* [en línia]. Acadèmia EITCA, 6 d’agost de 2023 [Consultat: 27 d’Abril de 2025]. Disponible a: https://ca.eitca.org/informaci%C3%B3-qu%C3%A0ntica/eitc-qi-qif-fonaments-de-la-informaci%C3%B3-qu%C3%A0ntica/introducci%C3%B3-a-la-computaci%C3%B3-qu%C3%A0ntica/n-sistemes-qubit/revisi%C3%B3-d'examen-n-sistemes-qubit/quin-%C3%A9s-el-concepte-de-superposici%C3%B3-en-mec%C3%A0nica-qu%C3%A0ntica-i-com-es-relaciona-amb-el-comportament-dels-qubits-en-un-sistema-de-n-qubits/
2. **BBC News Mundo.** *Max Planck, el padre de la teoría cuántica que intentó convencer a Hitler de que permitiera trabajar a los científicos judíos* [en línia]. BBC News Mundo, 23 d’abril de 2019 [Consultat: 30 d’abril de 2025]. Disponible a: https://www.bbc.com/mundo/noticias-48025060
3. **Bennett, C. H., & Brassard, G.** (1984). *Quantum cryptography: Public key distribution and coin tossing*. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175–179.
4. **Bohr, N.** (1928). *The quantum postulate and the recent development of atomic theory*. *Nature*, 121(3050), 580–590.
5. **Clarín.** *Explicación sencilla del gato de Schrödinger* [en línia]. Clarín, 20 de novembre de 2022 [Consultat: 27 d’abril de 2025]. Disponible a: https://www.clarin.com/viste/explicacion-sencilla-del-gato-de-schrodinger_0_RfEgmlSX0r.html
6. **Coluccio Leskow, Estefania.** *Mecánica cuántica* [en línia]. Enciclopedia Concepto, 24 d’octubre de 2024 [Consultat: 22 d’abril de 2025]. Disponible a: https://concepto.de/mecanica-cuantica/
7. **Einstein, A., Podolsky, B., & Rosen, N.** (1935). *Can quantum-mechanical description of physical reality be considered complete? Physical Review*, 47(10), 777–780.

8. **Escuela PCE.** *Resumen de la mecánica cuántica* [en línia]. Escuela PCE, data no disponible [Consultat: 22 d’abril de 2025]. Disponible a: https://escuelapce.com/resumen-de-la-mecanica-cuantica/
9. **Feynman, R. P., Leighton, R. B., & Sands, M.** (1965). *The Feynman Lectures on Physics, Vol. 3: Quantum Mechanics.* Addison-Wesley.
10. **García-Matos, Marta.** *El sentit quàntic IV: Per què?* Barcelona: Centre de Cultura Contemporània de Barcelona. [Consultat: 3 de maig de 2025]. Disponible a: https://lab.cccb.org/ca/el-sentit-quantic-iv-per-que/
11. **Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H.** (2002). *Quantum cryptography. Reviews of Modern Physics*, 74(1), 145–195.
12. **Greene, Jim.** *EPR paradox. EBSCO Research Starters*. [Consultat: 2 de maig de 2025]. Disponible a: https://www.ebsco.com/research-starters/physics/epr-paradox
13. **Heisenberg, W.** (1927). *Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. Zeitschrift für Physik*, 43(3–4), 172–198.
14. **Kragh, H.** (2000). *Quantum generations: A history of physics in the twentieth century.* Princeton University Press.
15. **La Reserva.** *Comprendiendo las diferencias entre la física clásica y la física cuántica* [en línia]. La Reserva, 13 de juny de 2023 [Consultat: 22 d’abril de 2025]. Disponible a: https://www.lareserva.com/diferencias_entre_fisica_clasica_y_fisica_cuantica
16. **Latorre, J. I.** (2017). *Cuántica: Tu futuro en juego.* Editorial Ariel.
17. **María, Francisco.** *Biografía y contribuciones de Edwin Schrödinger a la física cuántica* [en línia]. OK Diario, 21 de maig de 2025 [Consultat: 30 de Maig de 2025]. Disponible a: https://okdiario.com/ciencia/biografia-contribuciones-edwin-schrodinger-fisica-cuantica-14799161
18. **Martín Villafruela, J.** (2010). *Título del trabajo fin de grado.* Universidad de Valladolid. [Consultat: 20 de juliol de 2025]. Disponible a: https://uvadoc.uva.es/bitstream/handle/10324/60413/TFG-B.%202010.pdf?sequence=1
19. **Martínez, E.** (31/07/2025). *La luz tiene dos identidades, pero es imposible verlas a la vez.*

https://www.levante-emv.com/tendencias21/2025/07/31/luz-identidades-imposible-verlas-vez-120229002.html

20. **Pais, A.** (04/06/2020). *Física cuántica: qué es la dualidad partícula-onda de la luz y cómo su descubrimiento revolucionó la ciencia.* https://www.bbc.com/mundo/noticias-52815076
21. **Pastor, Julen.** *Física quàntica: L'experiment de la doble rendija* [en línia]. Dciencia, 28 de setembre de 2023 [Consultat: 27 d'abril de 2025]. Disponible a: https://www.dciencia.es/fisica-cuantica-el-experimento-de-la-doble-rendija/
22. **Paz, Juan Pablo.** (2007). *Einstein contra la mecánica cuántica: el azar, la ignorancia y nuestra ignorancia sobre el azar.* Buenos Aires: Departament de Física, FCEyN, UBA.
23. **Planas, Oriol.** *Física quàntica: què és i principis de la mecànica quàntica* [en línia]. Energia Nuclear, 21 de juny de 2023 [Consultat: 22 d'abril de 2025]. Disponible a: https://ca.energia-nuclear.net/fisica/quantica
24. **Redacció.** *Què és la decoherència quàntica i per què és clau per entendre el pas del món quàntic al clàssic* [en línia]. Noticias de la Ciencia, 16 de juny de 2025 [Consultat: 3 de maig de 2025]. Disponible a: https://noticiasdelaciencia.com/art/54233/que-es-la-decoherencia-cuantica-y-por-que-es-clave-para-entender-el-paso-del-mundo-cuantico-al-clasico
25. **Resueltoos.** *Efecto doble rendija* [en línia]. Resueltoos, 7 de març de 2024 [Consultat: 27 d'abril de 2025]. Disponible a: https://www.resueltoos.com/blog/fisica-y-quimica/efecto-doble-rendija
26. **Sánchez Cuevas, Gema; Sabater, Valeria.** *El principi d'incertesa de Heisenberg* [en línia]. *La Mente es Maravillosa*, 23 de desembre de 2018 [Consultat: 27 d'abril de 2025]. Disponible a: https://lamenteesmaravillosa.com/el-principio-de-incertidumbre-de-heisenberg/
27. **Schrödinger, E.** (1935). *The present situation in quantum mechanics. Proceedings of the American Philosophical Society.*
28. **Sectigo.** *RSA vs DSA vs ECC Encryption* [en línia]. Sectigo, data no disponible [Consultat: 20 de juliol de 2025]. Disponible a: https://www.sectigo.com/es/recursos/rsa-vs-dsa-vs-ecc-encryption

29. **Wikipedia.** *Distribución cuántica de claves* [en línia]. Wikipedia, data no disponible [Consultat: 24 de juliol de 2025]. Disponible a: https://es.wikipedia.org/wiki/Distribuci%C3%B3n_cu%C3%A1ntica_de_claves
30. **Wikipedia.** *Dualidad onda corpúsculo* [en línia]. Wikipedia, data no disponible [Consultat: 24 d'abril de 2025]. Disponible a: https://es.wikipedia.org/wiki/Dualidad_onda_corp%C3%BAsculo
31. **Wikipedia.** *Efecto túnel* [en línia]. Wikipedia, data no disponible [Consultat: 3 de maig de 2025]. Disponible a: https://es.wikipedia.org/wiki/Efecto_t%C3%BAnel
32. **Wikipedia.** *Entrelazamiento cuántico* [en línia]. Wikipedia, data no disponible [Consultat: 2 de maig de 2025]. Disponible a: https://es.wikipedia.org/wiki/Entrelazamiento_cu%C3%A1ntico
33. **Wikipedia.** *Erwin Schrödinger* [en línia]. Wikipedia, data no disponible [Consultat: 27 d'abril de 2025]. Disponible a: https://es.wikipedia.org/wiki/Erwin_Schr%C3%B6dinger
34. **Wikipedia.** *Gat de Schrödinger* [en línia]. Wikipedia, data no disponible [Consultat: 27 d'abril de 2025]. Disponible a: https://es.wikipedia.org/wiki/Gato_de_Schr%C3%B6dinger
35. **Wikipedia.** *Principi d'incertesa de Heisenberg* [en línia]. Wikipedia, data no disponible [Consultat: 27 d'abril de 2025]. Disponible a: https://ca.wikipedia.org/wiki/Principi_d'incertesa_de_Heisenberg
36. **Wikipedia.** *Python* [en línia]. Wikipedia, data no disponible [Consultat: 15 de juliol de 2025]. Disponible a: https://es.wikipedia.org/wiki/Python
37. **Wikipedia.** *Superposició quàntica* [en línia]. Wikipedia, data no disponible [Consultat: 27 d'Abril de 2025]. Disponible a: https://ca.wikipedia.org/wiki/Superposici%C3%B3_qu%C3%A0ntica
38. **Wikipedia.** *Teoría de variables ocultas* [en línia]. Wikipedia, data no disponible [Consultat: 3 de maig de 2025]. Disponible a: https://ca.wikipedia.org/wiki/Teoria_de_variables_ocultes
39. **Wikipedia.** *Thomas Young* [en línia]. Wikipedia, data no disponible [Consultat: 27 d'abril de 2025]. Disponible a: https://es.wikipedia.org/wiki/Thomas_Young

Annex

Codi del programa:

```
import random
import math

class BB84Simple:
    def __init__(self, n=50, eve_prob=0.0):
        self.n = n
        self.eve_prob = eve_prob
        self.measurements = 0

    def measure_quantum(self, bit, prep_base, meas_base):
        self.measurements += 1
        if prep_base == meas_base:
            return bit
        else:
            return random.randint(0, 1)

    def eve_attack(self, bit, alice_base):
        eve_base = random.randint(0, 1)
        eve_result = self.measure_quantum(bit, alice_base, eve_base)
        return eve_result, eve_base

    def run(self):
        print(f"BB84 - {self.n} qubits, Eva: {self.eve_prob*100:.0f}%")

        # Alícia prepara bits i bases aleatòries
        alice_bits = [random.randint(0, 1) for _ in range(self.n)]
        alice_bases = [random.randint(0, 1) for _ in range(self.n)]


        transmitted_bits = []
        transmitted_bases = []
        eve_count = 0

        for i in range(self.n):
            bit, base = alice_bits[i], alice_bases[i]

            if random.random() < self.eve_prob:
                bit, base = self.eve_attack(bit, base)
                eve_count += 1

            transmitted_bits.append(bit)
            transmitted_bases.append(base)
```

```
        bob_bases = [random.randint(0, 1) for _ in range(self.n)]
        bob_results = []

        for i in range(self.n):
            result = self.measure_quantum(transmitted_bits[i],
transmitted_bases[i], bob_bases[i])
            bob_results.append(result)


        sifted_alice = []
        sifted_bob = []

        for i in range(self.n):
            if alice_bases[i] == bob_bases[i]:
                sifted_alice.append(alice_bits[i])
                sifted_bob.append(bob_results[i])

        # Anàlisi de resultats
        if len(sifted_alice) == 0:
            print("Sense bits útils")
            return

        errors = sum(a != b for a, b in zip(sifted_alice, sifted_bob))
        error_rate = errors / len(sifted_alice) * 100
        efficiency = len(sifted_alice) / self.n * 100

        print(f"Eficiència: {efficiency:.0f}% ({len(sifted_alice)}/{self.n} bits)")
        print(f"Errors: {errors}, Taxa: {error_rate:.1f}%")
        print(f"Eva interceptà: {eve_count} qubits")

        if error_rate <= 11:
            print("SEGUR - Clau utilitzable")
        else:
            print("INSEGUR - Possible espia detectat")

        print(f"Alícia: {sifted_alice[:20]}")
        print(f"Bob:    {sifted_bob[:20]}")
        print()

def demo():
    print("Demo BB84")

    for i in range(3):
        n_qubits = random.randint(30, 200)
        eve_prob = random.uniform(0.0, 0.9)

        print(f"Execució {i+1}: {n_qubits} qubits, Eva {eve_prob*100:.1f}%")
        bb84 = BB84Simple(n=n_qubits, eve_prob=eve_prob)
        bb84.run()
```

```
def principio_cuantico():
    print("Principi quàntic")
    print("Preparar |+⟩ i mesurar en base rectilínia:")

    bb84 = BB84Simple()
    resultados = []

    for _ in range(1000):
        resultado = bb84.measure_quantum(bit=0, prep_base=1, meas_base=0)
        resultados.append(resultado)

    ceros = resultados.count(0)
    unos = resultados.count(1)

    print(f"Resultats: {ceros} zeros, {unos} uns")
    print(f"Probabilitats: {ceros/10:.1f}% zeros, {unos/10:.1f}% uns")
    print("Incertesa quàntica confirmada")
    print()

if __name__ == "__main__":
    demo()

    print("Exemple individual:")
    qubits = random.randint(40, 150)
    eva = random.uniform(0.05, 0.6)
    print(f"Qubits: {qubits}, Eva: {eva*100:.1f}%")

    bb84 = BB84Simple(n=qubits, eve_prob=eva)
    bb84.run()
```