

Memòries de Pràctiques en Empresa - Criptografia Quàntica
QuantumLab UB

Marina Ristol

Setembre 2020 - Juny 2021



UNIVERSITAT DE
BARCELONA

Facultat de Física

Tutors: Bruno Juliá, Carles Calero i Montserrat Guilleumas

Entrega: 8 de juliol de 2021

Índex

Introducció	1
1 Projecte	3
1.1 QuantumLab UB	3
1.2 Idea inicial	3
1.3 Resultat final	3
2 Metodologia	4
2.1 Organització	4
2.2 Programes utilitzats	4
3 Base teòrica	5
3.1 Criptografia quàntica	5
3.2 Xifrat	6
4 El joc	7
4.1 Objectius	7
4.2 Desenvolupament del joc	7
4.2.1 Procés general per obtenir la clau compartida aplicat al joc	8
4.3 Part gràfica: Pantalles	9
4.3.1 Inici	9
4.3.2 Jugant amb claus	10
4.3.3 Bob	11
4.3.4 Multijugador	14
5 Conclusions	16

Introducció

Aquestes memòries descriuen les pràctiques d'empresa fetes a *QuantumLab UB* durant el període del setembre del 2020 al juny del 2021. Les pràctiques han sigut tutoritzades pels professors Bruno Juliá, Carles Calero i Montserrat Guilleumas.

Primer de tot es presentarà el projecte a la secció (1) amb l'institució de *QuantumLab UB*. A continuació a la secció (2), es comenta la metodologia emprada enfatitzant en l'organització que s'ha seguit i els programes utilitzats. A la secció (3) s'explica la base teòrica física i a la secció (4) el desenvolupament del joc. Finalment, a la secció (5) es conclou.

1 Projecte

1.1 QuantumLab UB

El projecte de *QuantumLab UB* es va iniciar al febrer del 2018, supervisat per la Montserrat Guilleumas i en Bruno Juliá, amb l'objectiu d'apropar la física quàntica a un públic heterogeni. Els estudiants del grau de física desenvolupen programes de física quàntica que pretenen produir una eina útil per a la divulgació científica. Els/les estudiants col·laboren amb companys del mateix curs i tenen un seguiment dels tutors amb reunions setmanals on aprenen a exposar el seu treball realitzat. Per iniciar el projecte, se'ns va demanar que proposéssim un tema que fos un problema realista de la quàntica o bé un joc que el presentés.

1.2 Idea inicial

Inicialment vaig proposar fer un joc que fes entendre el procés de la criptografia quàntica. Al semestre anterior de començar les pràctiques, havia cursat l'assignatura de Mecànica Quàntica. El professor Lluís Garrido ens havia fet unes classes sobre comunicació quàntica, i específicament de la criptografia quàntica. Aquest tema em va atreure molt, però vaig trobar que tot el procés era difícil d'entendre si s'intentava explicar ràpidament. Per això, vaig pensar que seria un bon projecte fer un joc que intentés que un públic general pogués entendre aquest procés.

Hi ha dos personatges involucrats a la criptació quàntica, l'Alice i en Bob. Per tant, la idea era fer un joc que tingués un mode per cada un dels personatges i que la persona jugadora pogués triar ser una o l'altra. Cada mode seria un joc on s'ensenyaria el procés de la criptografia quàntica des del punt de vista de cada personatge.

1.3 Resultat final

Finalment he pogut desenvolupar un programa de criptografia quàntica, el primer que s'ha fet a *QuantumLab UB*. El programa té tres apartats; el primer s'anomena "Jugant amb claus" i no el tenia pensat fer inicialment. Tot i això, crec que és molt important per entendre la part del xifrat, que no és senzilla. El segon apartat és el d'en "Bob" i és el que ensenya tot el procés de la criptografia més o menys com tenia pensat a l'inici. La idea de fer l'últim apartat de "Multijugador" va aparèixer més

tard, com explico a la secció (4.2). Aquí s'aconsegueix fer la part del joc d'enviament i rebuda de partícules amb dues persones connectades des de la mateixa WiFi.

El projecte ha seguit sempre amb l'objectiu inicial de fer entendre el procés de la criptografia quàntica. Ha sigut enriquidor afegir dos apartats més al projecte aconseguint que s'entengués millor el xifrat i el procés general amb dues persones jugant.

2 Metodologia

2.1 Organització

L'equip està format pels tutors; Carles Calero, Montserrat Guilleumas i Bruno Juliá, i pels alumnes en pràctiques; Josep Bosch, Lluç Vayreda i jo. Ens vam organitzar de manera que fèiem una reunió setmanal on havíem d'exposar el treball que havíem anat avançant. Com que els alumnes en pràctiques anàvem treballant des de casa, aquestes reunions permetien als tutors fer un seguiment dels nostres projectes i guiar-nos. A nosaltres ens va ajudar molt poder fer-los-hi preguntes i veure les seves opinions. A més, les reunions ens han sigut molt útils per tenir objectius setmanals i pensar amb els avenços del projecte a curt plaç i organitzar-nos. També ens han servit per aprendre a fer exposicions i explicar els nostres treballs. Inicialment, com que no ho havíem fet gaire durant el grau, ens va costar fer-nos entendre bé a les reunions. A mesura que va anar passant el temps, vam anar agafant confiança en el projecte i amb nosaltres mateixos i ens va permetre fer unes reunions més dinàmiques i entenedores.

El fet de que fóssim tres alumnes de física, encara que estéssim involucrats en projectes diferents, també ens ha ajudat molt per poder resoldre dubtes entre nosaltres i poder-nos anar comentant els entrebancs.

Com que el període de pràctiques ha coincidit amb el COVID-19, totes les reunions les hem fet per *Meet*.

Des del principi del període de pràctiques, els tutors ens van avisar que segurament a final de curs, podríem participar a la Festa de la Ciència el 13 de juny. Per qüestions del COVID-19, dels tres alumnes en pràctiques, només va poder anar-hi en Lluç. Hagués sigut molt interessant per poder veure en pràctica el joc amb altra gent i observar si es complien els objectius proposats.

2.2 Programes utilitzats

Durant el període de pràctiques, hem après a utilitzar diverses eines i programes per desenvolupar i compartir el projecte.

Un d'ells ha sigut *GitHub*. En aquesta plataforma hi ha tots els projectes de *QuantumLab UB* i nosaltres hi hem afegit els nostres [1]. És una eina molt útil per compartir el codi i anar tenint un historial d'aquest sense perdre les versions anteriors. Cada setmana abans de fer la reunió penjàvem les actualitzacions del nostre codi a *GitHub* de manera que sempre estigués actualitzat. *GitHub* ens ha servit molt sobretot per baixar-nos els codis dels nostres companys i comprovar que funcionessin bé i també per extreure idees dels altres codis si en algun moment t'havies encallat amb el teu.

Els alumnes en pràctiques també hem anat fent una mena de diari, on hem anat explicant els nostres progressos, els entrebancs i les idees per desenvolupar. L'hem escrit en un document d'*Overleaf* que ens ha permès treballar i aprendre el *Latex*. Aquesta eina l'hem pogut aprofitar molt, ja que després al grau l'hem utilitzat tant en entregues i treballs com en el Treball de Fi de Grau. Al anar escrivint els diferents problemes al document, ens ha permès organitzar-nos i ordenar les idees per poder treballar millor.

El joc l'hem desenvolupat programant amb *Python* [2]. Anteriorment, a l'assignatura d'Informàtica i a l'optativa de Processament d'Imatge i Visió Artificial, ja havíem programat amb aquest llenguatge. També vam cursar Física Computacional, que va ser l'assignatura que ens va portar a aquestes pràctiques amb el professor Bruno Juliá, programant amb Fortran 77. Per tant, al principi ens vam haver de tornar a acostumar a aquest llenguatge. Fent el joc, vaig aprendre a treballar amb classes i objectes, que eren conceptes nous per mi, ja que els havíem d'utilitzar amb la llibreria *Kivy* [3]. Aquesta llibreria és la que hem utilitzat els alumnes que hem treballat amb *QuantumLab UB* per fer un entorn gràfic senzill i pràctic pel nostre joc. És de lliure accés i es pot trobar documentació seva per treballar-hi sense problemes. Pel seu funcionament, es necessiten dos fitxers: en el primer (.py) s'hi troben les funcions i tot el cos del programa i en el segon (.kv) és amb un llenguatge específic on s'escriu tota la part gràfica. Els dos fitxers es connecten i es passen informació a l'hora d'executar el joc. Per aprendre a utilitzar el *Kivy* van ser necessàries varies hores per l'aprenentatge i per acostumar-se a l'entorn. Tot i així, buscant per internet es poden trobar la solució a molts dubtes i problemes que es puguin tenir amb aquesta llibreria.

3 Base teòrica

3.1 Criptografia quàntica

Hi ha dues (o tres) persones involucrades: l'Alice que vol enviar un missatge i en Bob que el rep. També hi pot haver una tercera persona que intenti hackejar el missatge: l'Eva.

Per transmetre's informació, l'Alice i en Bob es passen partícules d'spin $1/2$. Si es mesuren amb un Stern Gerlach amb una direcció arbitrària donaran sempre resultat $+\hbar/2$ o bé $-\hbar/2$, que s'interpretarà com a 1 o 0 respectivament. Les partícules que s'envien són àtoms de plata, ja que tenen un sol electró de valència que determina el valor de l'spin i per tant aquesta part es comporta igual que la d'un electró sol.

En aquest mètode d'intercanvi d'informació es jugarà amb les direccions d'enviament i de mesura del Stern Gerlach. Si les dues direccions són la mateixa, l'Alice i en Bob obtindran els mateixos resultats. Si no són les mateixes, en Bob tindrà el 50% de probabilitat d'obtenir el mateix valor que ha enviat l'Alice.

La gràcia de tot aquest procediment és que un estat quàntic no es pot clonar ni mesurar sense pertorbar-lo. A més, en aquest cas, per mesurar l'estat s'ha de destruir. Per tant, si hi hagués una persona espia, al mesurar els estats enviats per l'Alice, els alteraria.

Els passos que s'ha de seguir per aconseguir una clau secreta compartida són:

1. L'Alice enviarà partícules d'spin $1/2$ amb resultat 0 o 1 en la direcció que ella prefereixi, alternat-

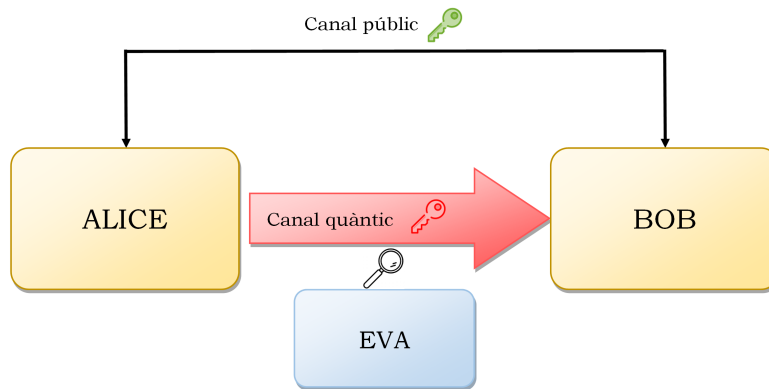


Figura 1: Esquema del procés de la criptografia quàntica explicat. La clau vermella representa la clau privada i la verda la pública.

ne dues, per exemple en l'eix z i en l'eix x i ho anotarà.

2. En Bob rebrà les partícules i per cada una decidirà en quina direcció la vol mesurar i anotarà els seus resultats.
3. L'Alice i en Bob compartiran les direccions en que han enviat/mesurat les partícules i descartaran les partícules que les hagin mesurat en direccions diferents, quedant-se amb els resultats de les partícules que els dos hagin mesurat en el mateix eix.
4. Compartiran una petita part (la mateixa els dos) dels resultats que han obtingut de la mesura. Si aquests resultats són iguals, vol dir que ningú els ha estat hackejant. Si n'hi ha molts de diferents (s'ha de posar un percentatge límit) significa que algú ha estat intentant espiar-los.
5. Si no hi ha hagut cap Eva, o sigui, cap persona que els ha intentat hackejar, els resultats (bits 0 o 1) que hauran obtingut, sense comptar la part que hauran fet pública, serà la seva clau compartida.
6. Un cop les dues persones ja tenen la clau, l'Alice ja pot encriptar el seu missatge i enviar-lo a en Bob perquè el pugui desxifrar.

3.2 Xifrat

La clau que s'obtindrà amb el procés explicat anteriorment, serà com a mínim de la mateixa longitud que el missatge que es vol transmetre [4]. Queda clar, doncs, que la informació que s'obté conjuntament entre l'Alice i en Bob, no és el missatge sinó la clau per desxifrar-lo.

El missatge que es vol fer arribar, primer de tot, s'ha de xifrar amb la clau obtinguda i després es publica. No passa res si algú més ho llegeix perquè està encriptat i no s'entén. Finalment en Bob el pot obtenir i desxifrar-lo amb la clau privada.

El xifrat que s'utilitza és el de la llibreta d'un sol ús [5]:

La clau consisteix en tants nombres com caràcters té el missatge, i cada nombre correspon a un caràcter: el primer número amb la primera lletra, el segon amb la segona... Llavors s'associa a cada lletra de l'abecedari un número (per exemple es pot fer amb el codi ASCII) i es tradueix el missatge original a números. Quan es té aquesta seqüència de números, se li suma la clau obtinguda en el procés d'enviament de partícules i es fa el mòdul perquè el número resultant quedi entre el mateix rang que el descrit inicialment. Ara ja es té el missatge encriptat que serà intel·ligible. Aquest serà el missatge que es farà públic. Finalment l'únic que ha de fer en Bob és prendre el missatge publicat i restar-li la clau secreta que han obtingut del procés (fent també el mòdul).

4 El joc

4.1 Objectius

L'objectiu d'aquest joc és que els/les participants puguin aprendre diferents conceptes de la mecànica quàntica com; l'spin, el col·lapse de la funció d'ona en la mesura i la impossibilitat de la clonació d'un estat per poder entendre la criptografia quàntica, o sigui, la teoria del mètode per obtenir una clau secreta entre dues persones sabent que no hi ha ningú que els pugui estar espiant.

4.2 Desenvolupament del joc

Primer de tot, vaig pensar quin xifrat havia d'utilitzar perquè sigués intuïtiu, però alhora no fos fàcil de desencriptar. Vaig optar al xifrat explicat a la secció (3.2) i vaig elaborar el programa amb python que encriptés i desencriptés missatges amb claus aleatòries. Un cop vaig haver après com anava la llibreria *Kivy*, vaig començar la part gràfica, afegint al joc dues pantalles sobre el procés de xifratge. Una amb una clau senzilla (d'un sol nombre per totes les lletres) i l'altre amb una clau tant llarga com caràcters tingui el missatge que es vulgui enviar. El contingut de les pantalles s'explica de manera més completa posteriorment.

Un cop vaig haver acabat el procés de xifratge, vaig començar a preparar el joc principal que ensenya el procés complet de la criptografia:

1. Procés d'enviament i rebuda de partícules
2. Obtenció de la clau privada
3. Encriptació i publicació del missatge
4. Rebuda i desencriptació del missatge

La meua primera idea va ser que el jugador fes del personatge d'en Bob i que l'Alice la programés jo. D'aquesta manera la persona jugadora rebria les partícules que l'Alice envia en dues direccions. Llavors publicarien totes dues les seves direccions i comprovarien si hi ha algú que els espia. Si no fos així, la persona que juga de Bob ja obtindria la clau secreta que utilitzaria per desxifrar el missatge que l'Alice li ha enviat. Per dur a terme aquesta part vaig invertir gran part de les hores pel projecte.

Em vaig trobar amb alguns problemes, com el de la gran quantitat de partícules que s'han d'enviar i rebre. Per enviar el missatge s'utilitza el codi binari. A cada lletra se li assigna un número, on cada

un té la seva representació de forma binària. El problema ve quan per enviar un missatge de dues paraules com “HI”, es necessiten enviar i rebre 30 partícules. El procés del joc pot ser una mica pesat, si en Bob hagués de rebre centenars de partícules. Vaig adaptar la pantalla i vaig fer que hi hagués l’opció per quan la persona jugadora es cansés, que pogués rebre directament totes les partícules que li faltessin amb direccions aleatòries.

Un altre problema amb el que em vaig trobar va ser al moment de compartir les direccions de cada partícula, ja que al joc s’ensenyen llistes de més de 30 elements. No quedava gaire estètic que al mig del joc hi hagués taules d’aquestes magnituds. A més, el *Kivy* no ofereix una manera senzilla d’ensenyar tantes dades. He optat per ensenyar les dades en format de text que es pogués desplaçar i hi cabés a la pantalla del joc. Es pot veure a la secció (4.3).

Quan vaig acabar la pantalla de “Bob”, un dels meus tutors em va donar una idea molt interessant: enlloc de fer una altra pantalla on la persona jugadora fes d’Alice, podria fer una pantalla on dues persones juguessin alhora a través d’internet. No hi havia cap projecte anterior que hagués treballat a través d’una xarxa i se’m presentava un gran repte. Al anar-hi dedicant hores, vaig aprendre com funcionava la connexió a internet a través del programa que havia anat creant. Aquesta és la pantalla de “Multijugador” i permet la connexió entre dues persones jugadores en ordinadors diferents, sempre que estiguin connectades a la mateixa xarxa WiFi. La part gràfica de la part del joc és pràcticament igual que la d’en “Bob”, però en aquest cas, hi ha un/a participant per cada personatge. Vaig començar aconseguint que les dues persones jugadores es connectessin a la mateixa partida, i que cada una veiés els moviments i les partícules que enviava l’altra. D’aquesta manera vaig intentar seguir el joc, intentant compartir les direccions de cada persona, però em vaig topar amb un altre problema. A l’hora d’executar el programa, m’apareixia l’error següent:

```
[WinError 10054] Se ha forzado la interrupción de una conexión existente por el
host remoto
```

Com que aquest error no em deixava continuar el procés del joc, hi vaig invertir molt de temps, revisant tot el codi, buscant solucions de l’error per internet... Com que no és un error “típic” i cap dels meus companys s’hi havia trobat, ja que no utilitzen l’internet, no vaig poder tenir gaire ajuda exterior per resoldre el problema. Vaig estar informant-me i aprenent més sobre la connexió amb internet a través de *Python*, però no vaig aconseguir resoldre-ho. Aquest error no m’havia sortit a la pantalla anterior, i em va estranyar molt, ja que el que passa, es que el joc es desconnecta i es tanca. Per això i per la falta de temps no vaig poder continuar el procés de “Multijugador”.

Tot i això, he après molt introduint la connexió a internet i la possibilitat de fer l’apartat del joc multijugador. M’hagués agradat tenir més temps per invertir-lo en solucionar aquest problema i poder acabar el procés.

4.2.1 Procés general per obtenir la clau compartida aplicat al joc

Primer de tot es necessita la longitud del missatge que es vol transmetre, per saber la llargada de la clau que s’ha de generar. Per obtenir aquesta longitud, el més fàcil és directament escriure el missatge. A partir de la longitud, ja es pot fer el procés per obtenir una clau compartida. A l’inici del procés, no

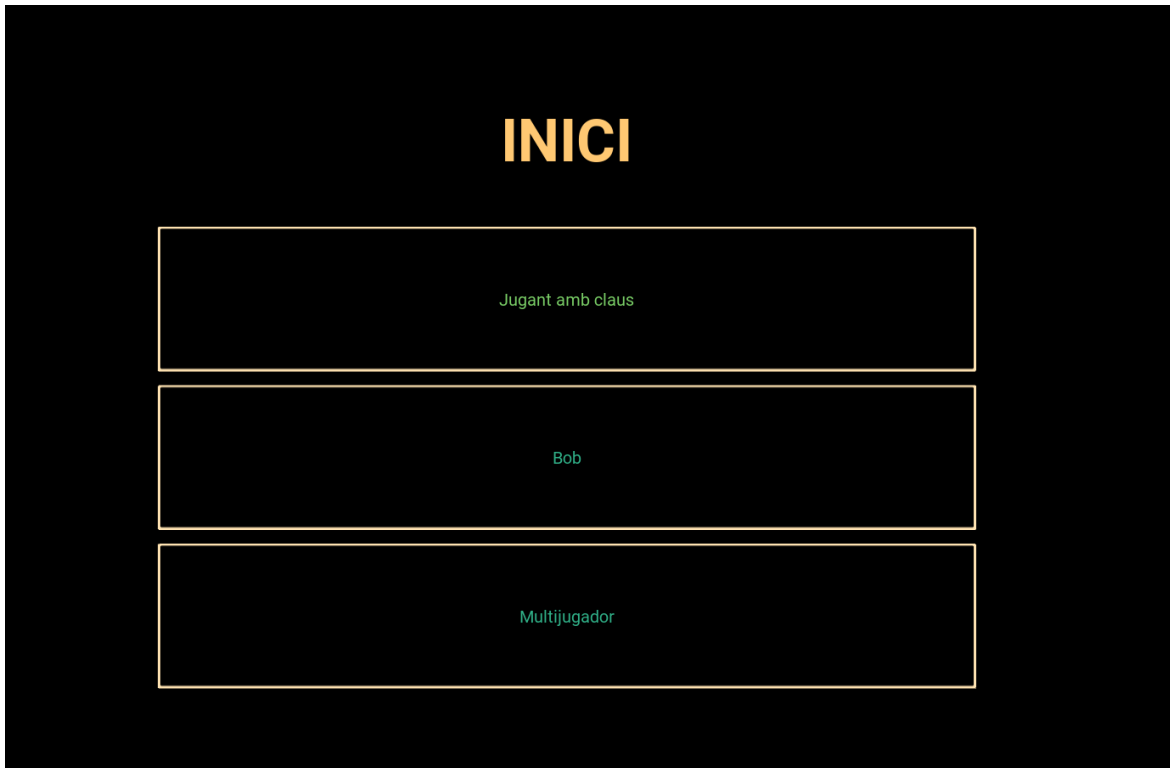


Figura 2: Pantalla d'inici

es pot saber de quina serà la longitud exacta de la clau obtinguda, per tant, si resulta ser més curta del que es necessita, es tornarà al fer el procés per obtenir més nombres. El procés d'enviar partícules (el de l'Alice) es basa en triar el valor del bit (0 o 1) i la direcció (z o x). Al joc també s'ha afegit, per fer-lo més dinàmic, que l'Alice i en Bob es poguessin moure amunt o avall. Llavors, en Bob pot escollir la direcció amb que rep la partícula que li envia l'Alice (també z o x).

A continuació, les dues persones publiquen les seves direccions per descartar els valors amb direccions diferents. A més, compartiran els valors dels bits d'unes partícules en concret, per veure que no hi hagi ningú que els espia, que no hi hagi cap Eva. Si veuen que no hi ha cap "hacker", ja tindran la seqüència de bits que forma la seva clau compartida! Llavors ja es pot encriptar el missatge i enviar-lo, perquè pugui ser rebut i finalment desencriptat amb la mateixa clau.

4.3 Part gràfica: Pantalles

4.3.1 Inici

A la Fig. 2 es pot veure la pantalla de l'inici. Es pot triar iniciar el joc amb les claus, fer el procés d'encriptació sent en Bob o bé jugar amb l'opció multijugador.

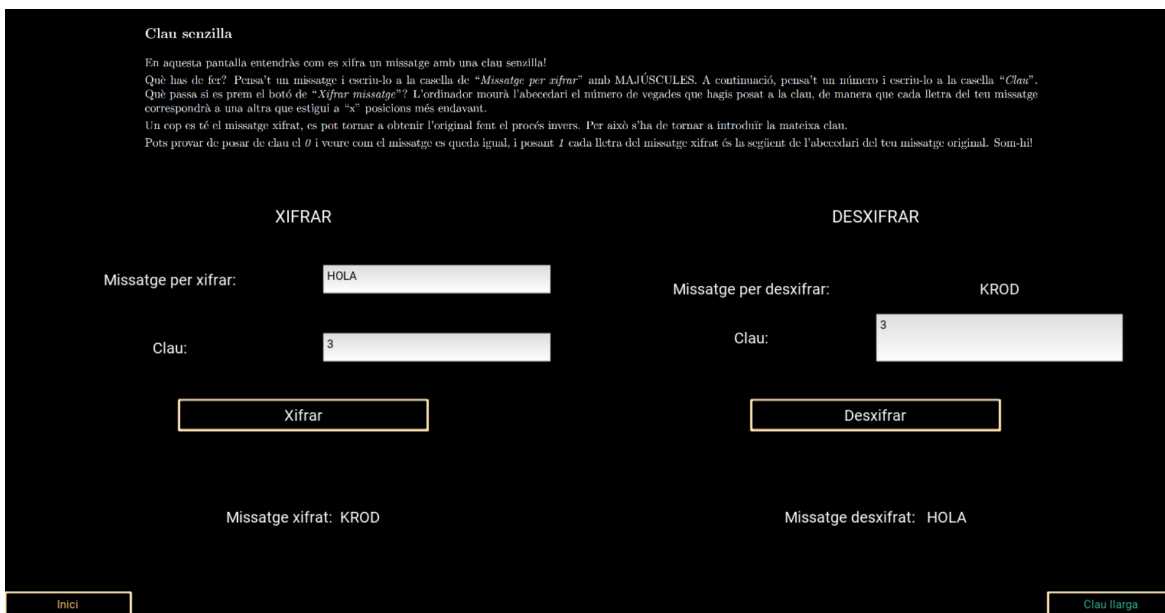


Figura 3: Pantalla de la clau senzilla

4.3.2 Jugant amb claus

- **Clau senzilla**

Les pantalles de "Jugant amb claus" tenen l'objectiu d'entendre la part del xifratge. En aquesta pantalla (Fig. 3), es demana que s'escrigui un missatge i un número. Amb aquestes dades es xifra el missatge enviat de manera que en queda un intel·ligible. En aquest apartat s'utilitza un xifrat més senzill que el que s'utilitza al joc: la clau utilitzada és la mateixa per cada caràcter del missatge (recordar com anava el xifrat a la secció (3.2)). Aquesta forma de xifrar no és gaire segura, ja que es podria hackejar fàcilment provant només 26 combinacions. Per xifrar de forma segura s'utilitza una clau amb un número per cada caràcter del missatge. És el que s'ensenya a la pantalla següent: Clau llarga.

Text d'explicació del joc:

En aquesta pantalla entindràs com es xifra un missatge amb una clau senzilla! Què has de fer? Pensa't un missatge i escriu-lo a la casella de "Missatge per xifrar" amb MAJÚSCULES. A continuació, pensa't un número i escriu-lo a la casella "Clau". Què passa si es prem el botó de "Xifrar missatge"? L'ordinador mourà l'abecedari el número de vegades que hakis posat a la clau, de manera que cada lletra del teu missatge correspondrà a una altra que estigui a "x" posicions més endavant de l'abecedari. Un cop es té el missatge xifrat, es pot tornar a obtenir l'original fent el procés invers. Per això s'ha de tornar a introduir la mateixa clau.

Pots provar que posant de clau 0 el missatge es queda igual, i posant 1 cada lletra és la següent de l'abecedari del teu missatge original. Som-hi!

- **Clau llarga**

Aquesta pantalla (Fig. 4) només demana escriure el missatge que la persona vulgui. Genera

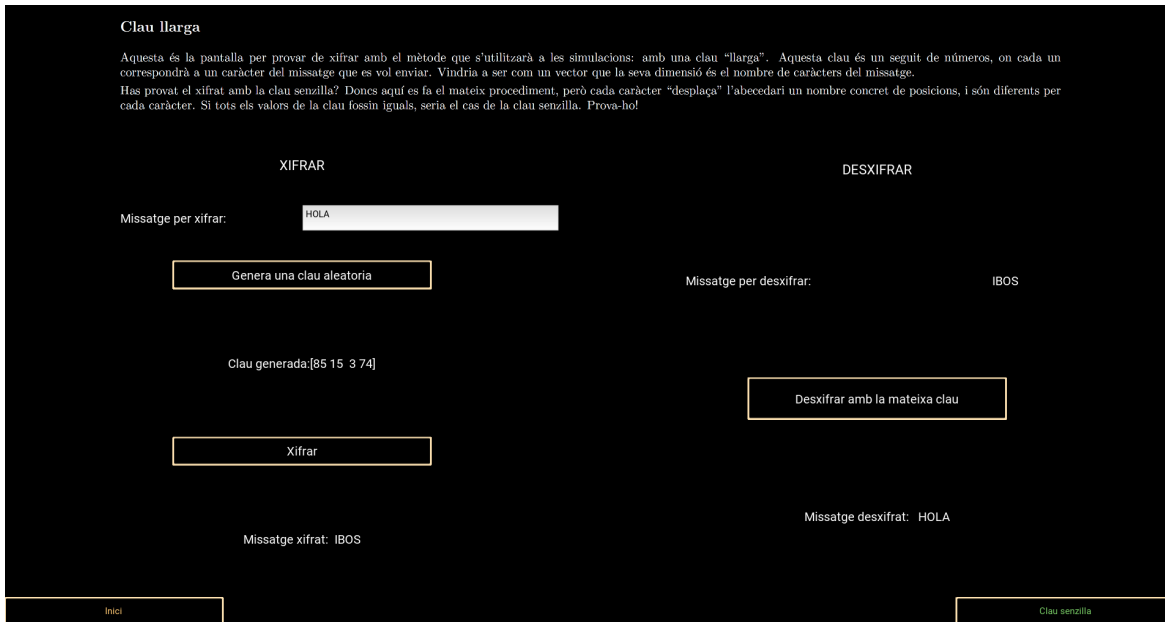


Figura 4: Pantalla de la clau llarga

automàticament una clau aleatòria: assigna un número a cada caràcter del missatge escrit. Tot el procés està descrit a la secció (3.2)

Text d'explicació del joc:

Aquesta és la pantalla per provar de xifrar amb el mètode que s'utilitzarà a les simulacions: amb una clau "llarga". Aquesta clau és un seguit de números, on a cada un li correspondrà un caràcter del missatge que es vol enviar. Vindria a ser com un vector amb dimensió el nombre de caràcters del missatge. Has provat el xifrat amb la clau senzilla? Doncs aquí es fa el mateix procediment, però cada caràcter es "desplaça" a l'abecedari un nombre concret de posicions i cada un és diferent per cada caràcter. Si tots els valors de la clau fossin iguals, seria el cas de la clau senzilla. Prova-ho!

4.3.3 Bob

La idea és que la persona que juga faci el paper d'en Bob: mesurar les partícules en dues direccions diferents i anar apuntant els resultats.

Les partícules arriben de l'esquerra i la persona jugadora podrà anar amunt i avall amb el seu "Stern Gerlach" per mesurar-les amb una direcció o una altra prement la fletxa amunt o la fletxa cap a la dreta del teclat (Fig. 6). A continuació podrà compartir les seves direccions i comprovar que no hi ha cap espia amb les dades que rebrà de l'Alice (Fig. 7). Finalment es podrà aconseguir la clau compartida i descriptar el missatge que envi l'Alice (Fig. 8).

Text d'explicació del joc

Benvolgut a la simulació d'en Bob!

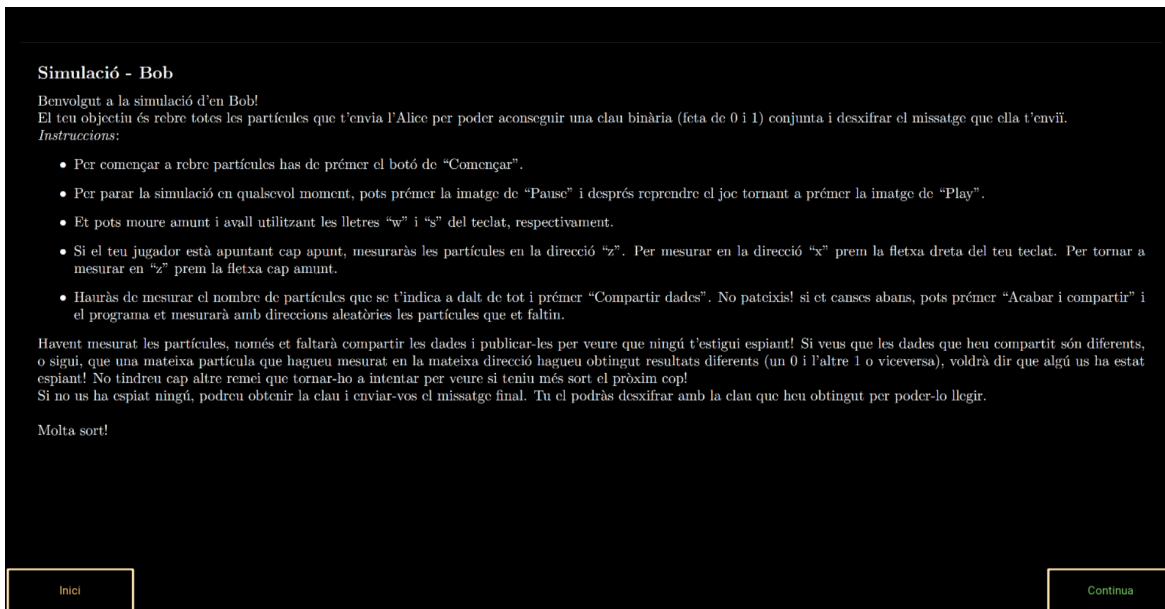


Figura 5: Pantalla d'instruccions d'en Bob

El teu objectiu és rebre totes les partícules que t'envia l'Alice per poder aconseguir una clau binària (feta de 0 i 1) conjunta i desxifrar el missatge que ella t'envia.

Instruccions:

- Per començar a rebre partícules has de prémer el botó de “Començar”.
- Per parar la simulació en qualsevol moment, pots prémer la imatge de “Pausa” i després reprendre el joc tornant a prémer la imatge de “Play”.
- Et pots moure amunt i avall utilitzant les lletres “w” i “s” del teclat, respectivament.
- Si el teu jugador està apuntant cap amunt, mesuraràs les partícules en la direcció “z”. Per mesurar en la direcció “x” prem la fletxa dreta del teu teclat. Per tornar a mesurar en “z” prem la fletxa cap amunt.
- Hauràs de mesurar el nombre de partícules que se t'indica a dalt de tot i prémer “Compartir dades”. No pateixis! Si et canses abans, pots prémer “Acabar i compartir” i el programa et mesurarà amb direccions aleatòries les partícules que et faltin.

Havent mesurat les partícules, només et faltaria compartir les dades i publicar-les per veure que ningú t'estigui espiaant! Si veus que les dades que heu compartit són diferents, o sigui, que una mateixa partícula que hagueu mesurat en la mateixa direcció l'Alice i tu rebeu resultats diferents (un 0 i l'altre 1 o viceversa), voldrà dir que algú t'ha estat espiaant! No tindreu cap altre remei que tornar-ho a intentar i a veure si teniu més sort el pròxim cop!

Si no us ha espiaat ningú, podreu obtenir la clau i enviar-vos el missatge final. Tu el podràs desxifrar amb la clau que heu obtingut.

Molta sort!



Figura 6: Pantalla d'enviament de partícules (Bob)

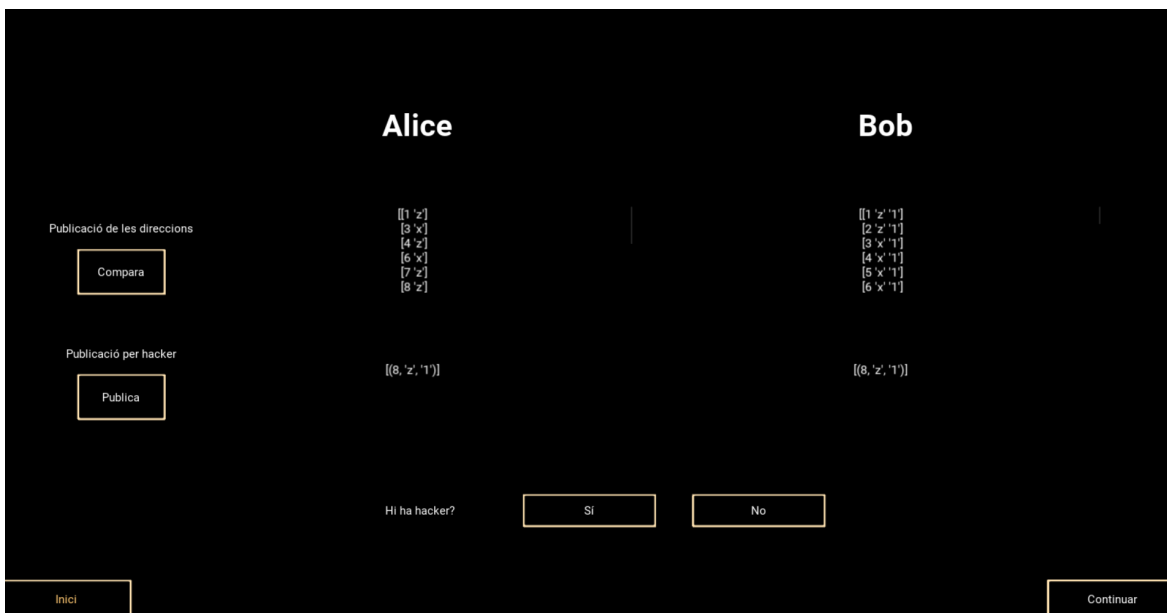


Figura 7: Pantalla per compartir les dades (Bob)

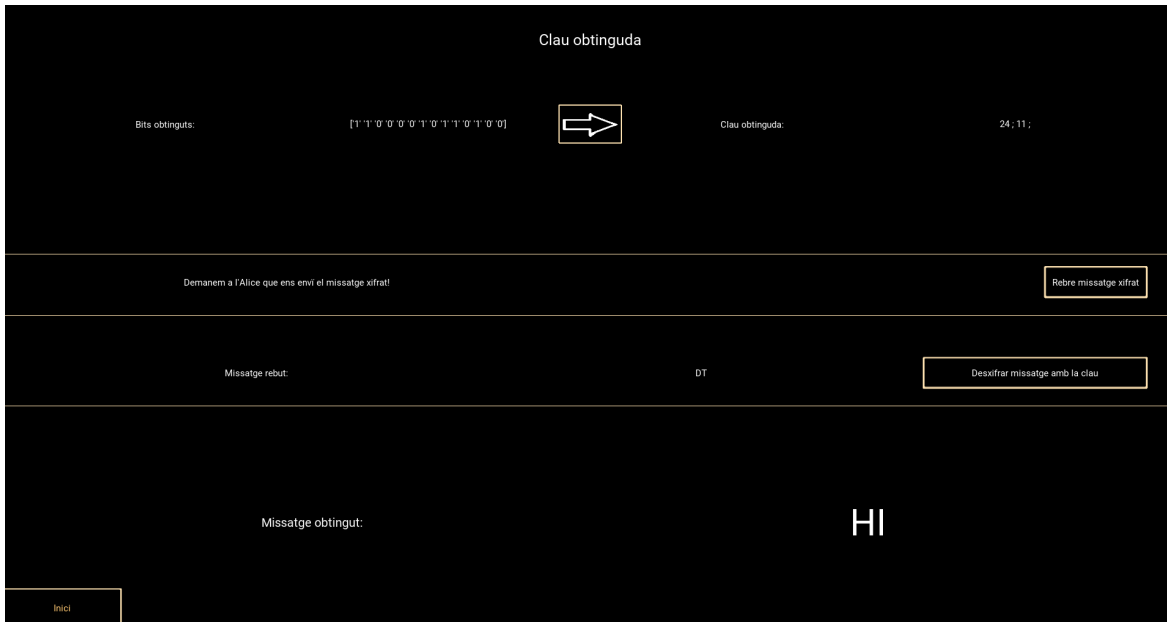


Figura 8: Pantalla per obtenir la clau (Bob)

4.3.4 Multijugador

Per jugar en aquest mode, es necessita connexió a internet. A part del programa del joc es necessita executar el programa de *server* per poder realitzar la connexió. Llavors el programa imprimeix per pantalla el valor del IP de la connexió WiFi que s’haurà de copiar per introduir-la a la pantalla inicial de multijugador. Això permetrà connectar-se a una partida compartida amb alguna altra persona del mateix WiFi (Fig. 9). Quan les dues jugadores estiguin connectades ja poden començar a jugar.

Llavors la persona que faci de Bob rebrà partícules de la mateixa manera que a la pantalla de “Bob” i l’Alice enviarà partícules prement el “0” o el “1” del teclat. També es pot moure amunt i avall amb les tecles “w” i “s”, respectivament, com en Bob (Fig. 10).

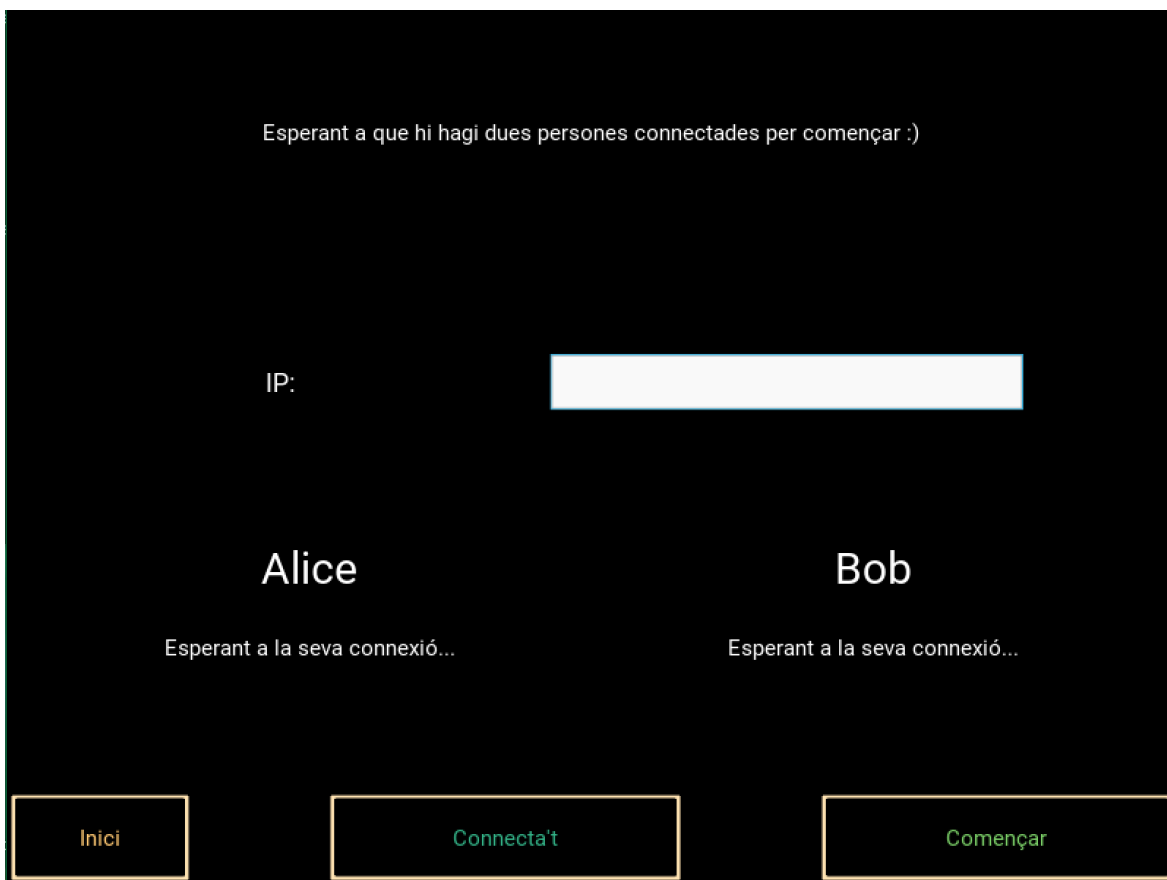


Figura 9: Pantalla de connexió (Multijugador)

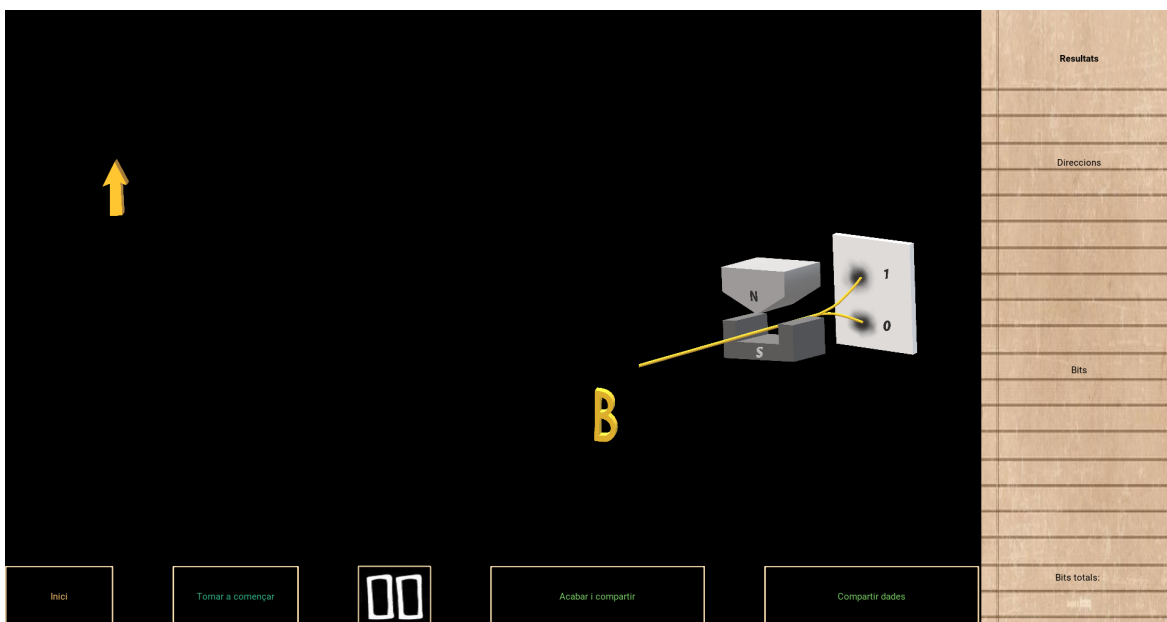


Figura 10: Pantalla de joc (Multijugador)

5 Conclusions

Aquestes pràctiques m'han sigut molt útils, primer de tot, per portar un projecte meu on he hagut d'aprendre pel meu compte. També he après a organitzar-me bé les hores de treball per anar avançant, encara que no tinguéssim cap horari establert. Fer les reunions setmanals amb els tutors i els companys ha sigut una gran experiència per poder anar fent exposicions del nostre projecte i aprendre a expressar-me amb claredat davant d'altres persones.

A més, el desenvolupament del projecte en sí, m'ha permès tenir molta més agilitat programant i poder conèixer conceptes i llenguatges nous aprenent-los totalment de manera autodidacta. Crec que seria molt interessant poder continuar el programa solucionant l'entrebanc en què m'he trobat. Fent el projecte sobre la comunicació quàntica obre una porta molt gran a *QuantumLab UB* i fins i tot, podria ser interessant que pròxims alumnes poguessin seguir en la línia d'aquest projecte i poder-lo acabar.

Referències

- [1] *GitHub - QuantumLab UB*
<https://github.com/brunojuliana/quantumlabUB>
- [2] Documentació de *Python*
<https://docs.python.org/3/index.html>
- [3] Documentació de *Kivy*
<https://kivy.org/doc/stable/api-index.html>
- [4] Idea del xifrat
Vídeo: Cómo Mandar un Mensaje Secreto con Física Cuántica — Encriptación Cuántica, QuantumFracture. Enllaç: <https://youtu.be/7R7dnT2043M>
- [5] Llibreta d'un sol ús
https://es.wikipedia.org/wiki/Libreta_de_un_solo_uso