Qiskit Fall Fest 2025

Jorge Giménez, Miguel Hernández, Andreu Moreno y Rubén Piles

9 de novembre de 2025

1 Per què ens interessa el problema?

El protocol BB84 és el primer cas pràctic de distribució quàntica de claus. Gràcies a la QKD, el problema de la seguretat incondicional queda, en teoria, resolt. No obstant això, obre la porta a diversos inconvenients que cal abordar. Nosaltres ens centrarem en les possibles vulnerabilitats i, concretament, en les que s'amaguen rere els errors dels sistemes amb què treballem.

2 Estat de la situació

2.1 Cas ideal de BB84

El protocol de QKD BB84 està bassat en el col.lapse de la funció d'ona. Els passos són els següents:

1. **Encoding**: Alice inicialitza aleatòriament un qubit en estat $|0\rangle$ o $|1\rangle$ i també tria la base (X o Z) aleatòriament.

2. **Canal clàssic**: l'estat s'envia per un canal clàssic, potencialment a llargues distàncies, fins arribar a Bob. Generalment s'empren fotons amb polaritzacions ortogonals i es propaguen per una fibra òptica. Aquesta fibra és la principal font de soroll (*noise*) però de moment ens centrem en el cas ideal.

3. **Decoding**: conforme arriben al receptor, els qubits són mesurats en la base X o Z, escollida aleatòriament, que pot coincidir o no amb la base escollida per Alice.

4. **Reconciliació**: Alice i Bob comuniquen per un canal públic quines bases han emprat per a fer les mesures. Cal destacar que aquesta informació no compromet, al menys a priori, la clau. Tan sols les mesures on Alice i Bob han escollit la mateixa base són emprades en la clau final. D'aquesta forma ens assegurem que la clau d'Alice i Bob és la mateixa.

5. **Pressència d'Eve**: en el cas de que un observador extern intercepte els qubits en el camí entre Alice i Bob, aquest col·lapsarà la seua funció d'ona al tractar de mesurar-los. Açò farà que, quan ALice i Bob comparen els seus resultats, no tinguen la mateixa clau. Per tant poden deduir la presència d'un tercer, i sabrán que la clau ha sigut compromesa. Cal destacar que aquesta discordància (*missmatch*) de les claus es pot deure també de forma indistingible a soroll, cosa que haurem de tractar més endavant.

3 Cas amb soroll

En el cas d'haver soroll, podem esperar que les claus de Alice i Bob no siguen exactament iguals, encara que no hi haja pressència d'un tercer (Eve). Per tant és important modelitzar el soroll per a estimar el seu abast. Posem per exemple que l'error del canal és d'un 10%, si el *missmatch* entre les claus d'Alice i Bob és inferior a aquesta quantitat, no podem afirmar la pressència d'Eve. En canvi, si es supera aquesta quantitat, molt probablement un tercer haja interceptat la connexió.

Si fem una simulació on avaluem la ràtio d'acceptació de claus (*key agreement rate*) per als casos **sense Eve i sense soroll**, **amb Eve i sense soroll**, **amb Eve i amb soroll**, i **sense Eve i amb soroll**; podem veure que distingir els casos amb soroll i/o Eve és quasi impossible, almenys fins al llindar de probabilitat de soroll de l'1%. Si augmentem aquest llindar al 10%, podem veure que a partir del 2% ja comencem a observar que el cas amb **només soroll** té pitjors ràtios que el cas **amb Eve**.

3.1 Ampliació de Privacitat

En el cas que el *mismatch* siga superior a l'error per soroll, no està tot perdut. Podem apicar una tècnica addicional, anomenada **ampliació de privacitat** per a reduir la informació que Eve té sobre la clau final. L'idea és la següent: Eve coneix tan sols una porció de la clau, aleshores apliquem un *hash*, que és un algoritme no invertible que transforma la nostra clau en una cadena (*string*) més curta. Aquests algoritmes estàn pensat per a donar resultats completament diferents per a dos *inputs* diferents, encara que aquests siguen molt semblants. Per tant, la clau final, emprada per Alice i Bob, serà molt diferent de la clau d'Eve, ja que, encara que aquesta conega el *hash* emprat per l'emissor i receptor, no pot inferir la clau completa.

3.2 Millores

Una potencial idea pot ser començar a emprar qubits lògics, en compte de qubits físics. Els qubits lògics estan compostos per 2 o més qubits físics. Generalment aquestos s'entrellaçen de forma que presenten informació redundant, la cual cosa els fa més resistents a errors. D'aquesta forma minimitzariem l'error del canal i per tant seriem més sensibles a atacs. No obstant, no ens queda clar quanta complexitat podria afegir al sistema i com de complicat ens seria identificar a un atacant.

Altres idees que hem considerat interessants de cara a un futur seria potenciar la caracterització de fonts de soroll, desenvolupar proves de seguretat robustes per als casos en entorns ruidosos i explorar les vies de certificació oficial (com les iniciatives de Nostradamus o Vigo Quantum) d'aquests sistemes per definir els models d'amenaces (*threat model*) de cada sistema.