# Ciberseguretat i vulnerabilitat en les telecomunicacions

## Criptografia clàssica *vs.* criptografia quàntica

**Miquel Tarzan***
Fundació Privada i2CAT, Internet i Innovació Digital a Catalunya
Miquel.Tarzan@i2cat.net

**Resum:** Els diversos avenços en el camp de la física quàntica dels darrers anys han fet que puguem tenir a l'abast, en un futur proper, els ordinadors quàntics. Aquests desenvolupaments tenen una enorme importància per a la criptografia. En aquest treball es dona una introducció a aquests temes: la computació clàssica i la quàntica, la criptografia i els efectes que la computació quàntica té en els seus algoritmes, i la nova criptografia quàntica. Es discuteix com els algoritmes clàssics de la criptografia estan en perill, i com d'altres basats en la física quàntica emergeixen amb un gran potencial per garantir la privacitat de les comunicacions.
**Paraules clau:** física quàntica, comunicacions quàntiques, criptografia, criptografia quàntica, algoritme BB84.

**Abstract:** In recent years, several advances in the field of quantum physics mean that quantum computers may be within reach in the near future. These developments are of enormous importance for cryptography. This paper provides an introduction to these topics: classical and quantum computation, cryptography and the effects that quantum computation will have on associated algorithms, and the new quantum cryptography. It discusses how classical cryptographic algorithms are endangered, and how others based on quantum physics have great potential to guarantee the privacy of communication.
**Keywords:** quantum physics, quantum communications, cryptography, quantum cryptography, algorithm BB84.

* Miquel Tarzan és llicenciat en Física i màster en Enginyeria Electrònica per la Universitat de Barcelona. Ha treballat en el camp de la intel·ligència artificial i la computació neuromòrfica aplicada a l'olfacció artificial en el marc de diferents projectes europeus. També ha treballat en el desenvolupament de noves arquitectures per a xarxes de telecomunicacions. Actualment, els seus àmbits d'interès són la intel·ligència artificial i les xarxes de comunicacions quàntiques. ORCID: orcid.org/0000-0003-3019-0952.

## Introducció

És difícil exagerar la importància que té la seguretat de les comunicacions en el dia a dia de la societat hiperconnectada en què vivim. Una societat com la nostra ens ofereix un conjunt gairebé il·limitat de possibilitats per relacionar-nos amb els altres, però aquestes possibilitats al mateix temps ens exposen a una gran quantitat de perills. Val la pena enumerar-ne uns quants, ja que els dedicarem la nostra atenció en les pàgines següents. Estem exposats a riscos associats a la confidencialitat de les nostres comunicacions, és a dir, volem que els missatges intercanviats entre nosaltres siguin secrets. Hi ha riscos de ser suplantats, amb la falsificació de missatges que semblen enviats per nosaltres sense saber-ho. Relacionat amb aquest risc hi ha la possibilitat que el nostre missatge sigui alterat. I, finalment, parlarem del risc de ser enganyats pels nostres interlocutors.

Aquests riscos s'entendran millor amb un exemple: imaginem que volem enviar un pagaré a un interlocutor a canvi d'un servei que volem rebre. Hem de garantir que ningú pugui esbrinar el contingut del pagaré, quantitat o servei pel qual pagarem; hem de garantir que ningú es pugui fer passar per nosaltres; no volem que ningú alteri el nostre pagaré, canviant-ne per exemple la quantitat a pagar; finalment, si som nosaltres els receptors del pagaré, volem estar segurs que l'emissor no es desdirà del pagament. Els termes tècnics per a aquestes condicions són confidencialitat o privacitat, autenticació, integritat i no rebuig. La taula I resumeix aquests termes.

En els propers apartats analitzarem com aquestes propietats són garantides per la criptografia clàssica i fins a quin punt, i els efectes que sobre aquests algoritmes té la nova computació quàntica. Començarem fent unes pinzellades de computació clàssica i quàntica, seguirem amb una anàlisi de la criptografia clàssica i les seves limitacions en un món d'ordinadors quàntics i finalment donarem una introducció a la criptografia quàntica amb un exemple d'algoritme.

## Computació clàssica i computació quàntica

A continuació donem una visió general de la computació clàssica i quàntica, amb un èmfasi especial en les diferències.

La computació clàssica es basa en sèries definides d'operacions sobre unes unitats mínimes d'informació, els anomenats bits. Un bit clàssic pot trobar-se en un de dos estats perfectament definits: l'estat 0 i l'estat 1.

Les operacions que es poden aplicar són les ben conegudes operacions lògiques: la negació —que és una operació que actua sobre un únic bit—, l'operació O (OR en anglès), l'operació I (AND en anglès), més una operació de còpia, que ens permet assignar l'estat d'un bit a un altre bit.

La computació quàntica (Kirsch, 2015) difereix de la clàssica en aspectes fonamentals. La mateixa definició de la unitat mínima d'informació és marcadament diferent. Aquesta unitat mínima, anomenada bit quàntic o qbit, pot estar en tres tipus d'estats: en l'estat 0, en l'estat 1, o —i aquí trobem la clau de la computació quàntica— en el que s'anomena una superposició de l'estat 0 i l'estat 1. Això vol dir, ni més ni menys, que un qbit pot estar simultàniament en els dos estats, 0 i 1. Una famosa interpretació d'això és l'anomenat gat de Schrödinger.

Aquesta propietat dels qbits permet operar simultàniament sobre els dos estats. Podem imaginar que fer operacions sobre els dos possibles estats ens in-

| Servei | Esquema | Tipus | Algoritmes |
|---|---|---|---|
| Privacitat | Xifratge | Clau simètrica, clau pública | AES, RSA |
| Autenticació | Signatura digital | Clau pública | SHA-256 |
| Integritat | Signatura digital | Algoritme de resum | SHA-256 |
| No rebuig | Centre de confiança | Clau pública | RSA |

**Taula I. Serveis i tipus de sistemes criptogràfics, i exemples dels algoritmes que els implementen.**

crementa el nombre d'operacions simultànies i, per tant, disminueix dràsticament el temps de computació. No és, però, l'únic avantatge —més endavant en veurem exemples.

Els bits i els qbits comparteixen les operacions lògiques, si bé amb una forma peculiar d'actuar sobre els qbits: com ja hem dit, les operacions sobre qbits actuen simultàniament sobre tots els estats en què es pot trobar.

Hi ha, però, una operació clàssica que no té equivalent quàntic: la còpia d'un qbit en un altre qbit. Aquesta és una característica fonamental dels estats quàntics, ja que els estats quàntics no es poden copiar o clonar. Aquest fet és d'una importància cabdal per a la criptografia quàntica, com veurem més endavant.

Aquesta propietat està relacionada amb una altra característica dels estats quàntics: mesurar-los és modificar-los. Un qbit pot estar en una superposició d'estats 0 i 1, però, si mesurem aquest estat, només obtindrem un 0 o un 1; i el qbit passarà a trobar-se en un estat quàntic pur de 0 o 1. La mesura altera, doncs, l'estat del qbit, i això fa que en el món quàntic no pugui existir, ni tan sols com a hipòtesi, l'espia perfecte: espiar un missatge és alterar-lo, i aquesta alteració deixarà una traça que es podrà detectar.

A part de les operacions lògiques, els qbits tenen altres operacions pròpies que no disposen d'equivalent en computació clàssica. Una d'aquestes característiques sense equivalent clàssic és l'anomenat entrellaçament quàntic (Jozsa, 1997). Consisteix a tenir dos qbits amb els seus estats lligats de tal manera que la mesura d'un d'ells ens informa de l'estat de l'altre, per lluny que aquests qbits es trobin. Encara que podria semblar que això implica una comunicació a velocitat superlumínica si els qbits es trobessin molt allunyats, no és el cas. No entrarem, però, en la discussió d'aquest tema.

## Fonaments de criptografia

Els elements bàsics necessaris per a la protecció de les comunicacions, sintetitzats a la taula I, són els algoritmes de xifratge, de signatura digital, i les funcions resum (*hash*). Ara aprofundirem en aquests conceptes. Tenim dos grans grups d'algorismes de xifratge: els simètrics i els asimètrics. Els simètrics es basen a aconseguir que l'emissor d'un missatge i el seu receptor comparteixin una clau secreta que utilitzen per xifrar i desxifrar els missatges. Les claus són seqüències de nombres aleatoris, i un algorisme per generar-los és, doncs, una condició prèvia per a aquests sistemes criptogràfics. En computació clàssica, aquests generadors de nombres aleatoris no són perfectes, ja que són en realitat algoritmes deterministes que donen l'aparença d'aleatorietat.

El que s'ha de resoldre en aquests algoritmes és com distribuir la clau secreta de forma eficient i eficaç per mantenir-la secreta, però un cop distribuïda, sota certes condicions en què no entrarem, aquests algoritmes són invulnerables. Com veurem a continuació, un algoritme asimètric ens pot resoldre la tasca de distribuir les claus.

Els algoritmes asimètrics, o algoritmes de clau pública (Paar i Pelzl, 2010), es basen en la dificultat computacional inherent a determinades operacions matemàtiques. Com veurem, aquest és un punt feble que la computació quàntica pot explotar per fer-los vulnerables. Per xifrar i desxifrar s'utilitzen dues claus: una de pública i una de privada —i d'aquí prové el nom d'algoritmes de clau pública. Aquesta clau pública és la que ens permet xifrar missatges i la privada, desxifrar-los. Alguns exemples paradigmàtics són el criptosistema RSA (pel nom dels seus autors: Ronald Rivest, Adi Shamir i Leonard Adleman), fonamentat en la dificultat de factoritzar en producte de nombres primers un de sencer molt gran, i el criptosistema de Diffie-Hellman, que es fonamenta en la dificultat de calcular el logaritme discret d'un nombre sencer molt gran.

Una dificultat d'aquests algoritmes es troba en el seu cost computacional, mesurat en nombre d'operacions, per fer els càlculs associats. Per mitigar aquest inconvenient, aquests algoritmes s'utilitzen en conjunció amb algoritmes simètrics, ja que són més directes, complementant-los (Paar i Pelzl, 2010). El mecanisme consisteix a crear el que s'anomena una sessió, el context en què s'utilitza un algoritme de clau pública per distribuir una clau secreta, que és la que ens permetrà xifrar i desxifrar els missatges.

Els algoritmes d'autenticació es basen en l'ús de la clau privada per signar un missatge, mentre que la clau pública permet comprovar la identitat de l'emissor del missatge.

La figura I mostra un exemple de privacitat i de signatura digital.

## Computació quàntica i criptografia clàssica

Els computadors quàntics fan vulnerables alguns dels criptosistemes més utilitzats (Kirsch, 2015).

Estudiarem ara dos algoritmes quàntics que tornen vulnerables algoritmes clàssics de criptografia. Hem de tenir en compte que aquests algoritmes són possibles gràcies a les propietats quàntiques que hem introduït en el segon apartat, i no tenen, per tant, equivalent clàssic.

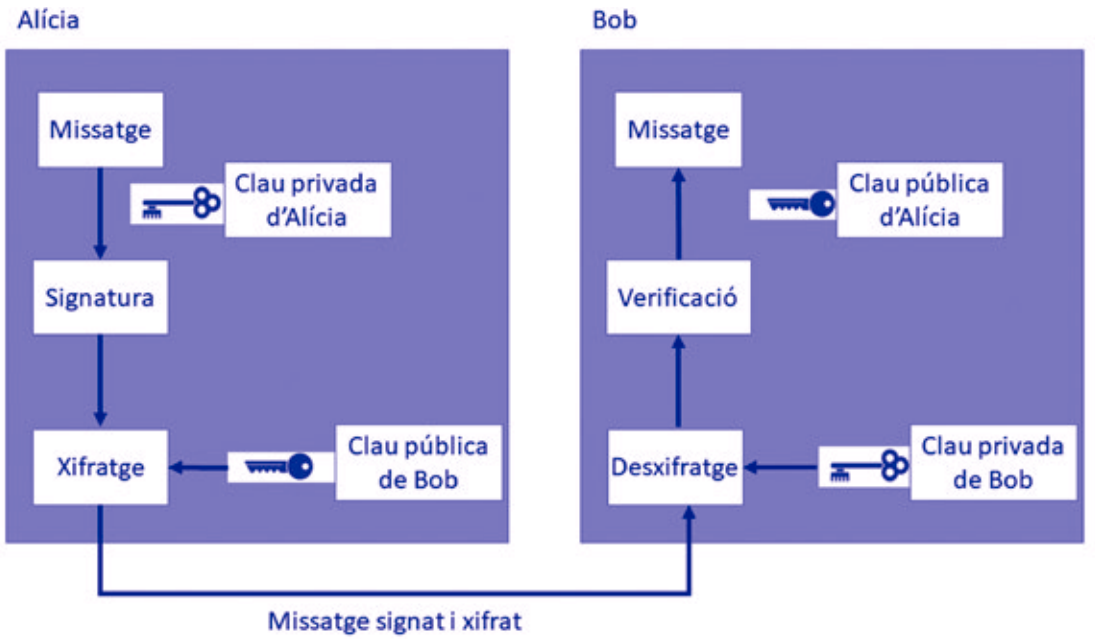


**Figura I. La clau privada de l'Alícia s'utilitza per signar el missatge, mentre que la clau pública d'en Bob és la que s'utilitza per xifrar-lo, i viceversa: la clau privada d'en Bob permet desxifrar el missatge amb la signatura, i la clau pública de l'Alícia permet verificar l'autoria del missatge.**

El primer és l'anomenat algoritme de Shor. No entrarem en els detalls tècnics, però podem dir que s'utilitza per donar la solució al problema de factoritzar un nombre sencer mitjançant una superposició d'estats. El resultat s'obté en un temps molt inferior al que necessitaria la computació clàssica. Els algoritmes criptogràfics asimètrics que estan basats en la dificultat d'aquesta factorització es tornen, doncs, vulnerables, com l'algoritme RSA i criptosistemes com el de Diffie-Hellman.

El segon algoritme és el de Grover, útil per fer cerques en una base de dades desordenada. Aquest és un problema difícil per a la computació clàssica, però amb la computació quàntica es pot portar a terme en un temps molt més curt.

Uns altres algoritmes vulnerables amb criptografia quàntica són les funcions resum. Utilitzant l'algoritme de Grover és factible trobar dos missatges amb el mateix resultat de la funció resum. D'aquesta manera es pot crear un missatge fals a partir d'un missatge autèntic amb el mateix valor de la funció resum.

## Criptografia quàntica

Però la criptografia quàntica ens dona també noves eines per protegir-nos, amb nivells de seguretat molt més alts, garantits pels mateixos fonaments de la física (Campagna *et al.*, 2015).

La física quàntica també ens proporciona algoritmes criptogràfics molt més fiables, ja que la seguretat és garantia pels seus fonaments. Ens centrarem en un algoritme per a la distribució segura de claus, requisit per a la criptografia simètrica. Es tracta de l'algoritme de Bennett i Brassard del 1984 (BB84) (Bennett i Brassard, 1984). El fonament d'aquest algoritme es troba en la representació del 0 i l'1 amb dos sistemes per codificar-los en qbits i per mesurar-los. Aquests dos sistemes es trien de tal manera que, si mesurem amb un sistema un estat codificat amb l'altre sistema, el resultat és un 0 o un 1 obtingut aleatòriament. És a dir, es perd la informació que s'havia codificat.

La taula II (vegeu la pàgina següent) ens mostra com es codifiquen el 0 i l'1 amb els dos sistemes; la taula III, els diferents resultats de mesurar els qbits amb els dos sistemes, i la taula IV, un exemple d'ús de l'algoritme BB84, que descriurem tot seguit.

| | 0 | 1 |
|---|---|---|
| **Sistema A** | ← | → |
| **Sistema B** | ↑ | ↓ |

**Taula II. Codificació del 0 i l'1 amb els dos sistemes de representació.**

| | **Mesurat amb A** | **Mesurat amb B** |
|---|---|---|
| ← | 0 | Resultat aleatori |
| → | 1 | Resultat aleatori |
| ↑ | Resultat aleatori | 0 |
| ↓ | Resultat aleatori | 1 |

**Taula III. Resultats de mesurar els qbits amb els diferents sistemes.**

| Llista de 0 i 1 aleatoris | 0 | 0 | 1 | 1 | 1 | 1 | 0 |
|---|---|---|---|---|---|---|---|
| Sistema de codificació | A | A | A | B | A | B | B |
| Qbits | ← | ← | → | ↓ | → | ↓ | ↑ |
| Sistema de lectura | A | B | A | B | B | A | B |
| Resultat de lectura | Sí | No | Sí | Sí | No | No | Sí |
| Bits de la clau | 0 | | 1 | 1 | | | 0 |

**Taula IV. Exemple de funcionament de l'algoritme BB84, en cada filera representa un dels passos necessaris per aconseguir distribuir la clau secreta entre l'Alícia i en Bob.**

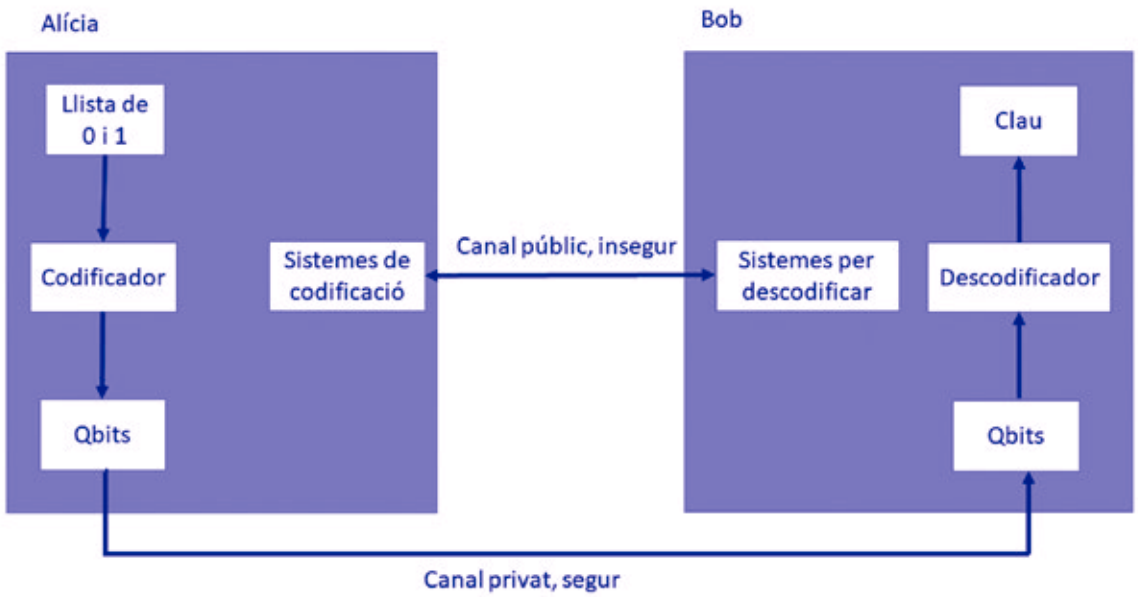


**Figura II. Esquema del dispositiu experimental per implementar l'algoritme BB84.**

En codificar el 0 i l'1 amb els dos sistemes de codificació escollits aleatòriament tenim una sèrie de qbits que podem transmetre.

A la figura II hi ha un exemple de dispositiu experimental per implementar aquest algoritme descrit a la taula IV. A la primera filera d'aquesta taula tenim una seqüència de 0 i 1 que volem transmetre per formar la clau secreta. La segona filera és una seqüència aleatòria de A i B que indica amb quin sistema es codifiquen els 0 i 1 de la primera filera. La tercera conté els qbits així codificats, que són els que transmetrà l'Alícia amb el canal privat i segur (figura II). La quarta filera és la llista de mesuradors A i B que utilitza en Bob per descodificar els qbits. Aquesta filera es fa pública amb un canal no necessàriament segur, i l'Alícia, utilitzant el mateix canal, indica a en Bob quins mesuradors són els que coincideixen (cinquena filera). A la sisena, agafant només els bits que han estat codificats i descodificats amb el mateix sistema, tenim els 0 i 1 de la clau. Alguns d'aquests bits es faran públics amb el canal no segur. Si hi ha errors en aquesta llista voldrà dir que algú ha espiat la transmissió dels qbits, ja que, com hem vist, mesurar és alterar; aleshores, la clau es descartaria.

L'algoritme BB84 té algunes limitacions i n'examinarem dues. La primera és evident a la taula IV: s'han descartat molts bits, i això sense comptar els que es fan públics per verificar que no hi ha hagut interferències al canal privat. Existeixen refinaments d'aquest algoritme per aprofitar millor els qbits, però no hi entrarem perquè cauen fora de l'abast d'aquest article.

La segona dificultat rau en el canal privat. Un tipus de canal que s'utilitza és la fibra òptica, però aquest sistema de transmissió té un abast màxim de centenars de quilòmetres. Per arribar més lluny s'hauria d'utilitzar algun tipus d'amplificació, però l'amplificador pertorbaria els qbits com ho faria un intrús. Un altre tipus de mitjà per transmetre qbits és el làser, i val la pena mencionar-lo perquè aquest any 2020 s'ha reportat la transmissió de claus entre dues localitzacions separades per 1.200 km amb un làser situat en un satèl·lit i fotons entrellaçats.

## Conclusions

En aquest article hem donat una visió panoràmica de les bases de la criptografia, en especial d'aquells elements que es veuen afectats per la nova computació quàntica. No hem discutit l'impacte que tenen aquests canvis en les bases sobre esquemes que les utilitzen, com ara les diferents capes d'internet. Hem vist elements bàsics de la computació clàssica i quàntica, de la criptografia i de la criptografia quàntica, amb un exemple realista d'un tal algoritme, l'algoritme BB84, i hem mostrat les seves limitacions i algunes formes de superar-les.

Amb els conceptes introduïts podem preguntar-nos l'impacte que la computació quàntica pot tenir en diferents tecnologies, com ara l'impacte per al *blockchain* i les criptomonedes. En principi, no hi ha res que impedeixi que s'hi introdueixin nous estàndards de seguretat a prova de desenvolupaments quàntics. Tot i això, no existeix ara per ara un esforç coordinat per impulsar aquests nous estàndards que substitueixin, per exemple, l'Elliptic Curve Digital Signature Algorithm, que és una de les tecnologies més vulnerables en la computació quàntica (Campbell, 2019), i això és un risc que no s'hauria de menystenir.

## Bibliografia


Bennett, C. H.; Brassard, G. (1984). «Quantum Cryptography: Public Key Distribution, and Coin-Tossing». A: *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Dec. 9-12, 1984, Bangalore, India*, pàg. 175-179.

Campagna, M. *et al.* (2015). *Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges* [en línia]. ETSI White Papers, 8. https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf [Consulta: 23 de juny de 2021].

Campbell, R. (2019). «Evaluation of Post-Quantum Distributed Ledger Cryptography». *The Journal of the British Blockchain Association*, vol. 2, núm. 1 (març), pàg. 7679.

Jozsa, R. (1997). «Entanglement and Quantum Computation». A: Hugget, S. *et al.* (eds.). *Geometric Issues in the Foundations of Science*. Oxford: Oxford University Press.

Kirsch, Z. (2015). *Quantum Computing: The Risk to Existing Encryption Methods*. Massachusetts: Tufts University. [Tesi doctoral]. http://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf [Consulta: 23 de juny de 2021].

Paar, C.; Pelzl, J. (2010). «Introduction to Public-Key Cryptography». A: *Understanding Cryptography*. Berlín, Heidelberg: Springer Berlin Heidelberg, pàg. 149-171.