Recentment, la Real Acadèmia de Ciències de Suècia, ha distingit amb el Premi Nobel de Física a tres investigadors en el camp de la Mecànica Quàntica: el francès Alain Aspect, l'estatunidenc John F. Clauser i l'austríac Anton Zeilinger. El premi ha estat concedit per "experiments d'avantguarda amb els estats quàntics entrellaçats···" experiments que "assenyalen el camí per a una nova tecnologia basada en la informació quàntica", i que per això cobreixen "un ampli camp d'investigació que inclou les computadores quàntiques, les xarxes quàntiques i la comunicació quàntica amb encriptats segurs", subratlla en la seua nota de premsa l'Acadèmia de Ciències sueca.

Per una altra banda, hi cal dir que el 2016 una part de la comunitat científica presenta un document, el Quantum Manifesto, " recolzat per una àmplia comunitat d'indústries, instituts de recerca i científics a Europa, document que va acompanyat d'una llista de milers de signataris" (3.400 segons els promotors), en el què hom fa una crida d'atenció als governs i al món de la indústria sobre el potencial de les tecnologies quàntiques al temps que proposa la inversió per implementar-les en suport a la transformació tecnològica que, segons els promotors, ja s'hi estava produint.

Però, pel que fa a la Criptografia hi cal dir:

1. Que no existeix Criptografia Quàntica. Que el que hi ha són dos protocols de distribució de la Clau de Xifrat d'un sol ús, protocols (BB84, E91 i variacions d'aquests) que deriven directament del Principi d'Indeterminació de Heisenberg o de la Monogàmia de l'Entrellaçament Quàntic. Aquesta clau criptogràfica ha de ser usada una sola vegada en el mètodes criptogràfics coneguts com one-time pad (Xifrat de Vernam) per tal que la comunicació entre l'emissor i el receptor hi siga absolutament segura.

2. Que la Criptografia Moderna (o de Shannon) no permet la invenció de criptosistemes Perfect Secrecy, perquè en aquest marc teòric la relació entre les cardinalitats dels conjunts dels Missatges M, dels Criptogrames C i de les Claus de xifrat K és:
$Card(C)>Card(M)>Card(K)$.

3. Que per ara només la Criptografia Aleph-0, permet construir infinitat de criptosistemes Perfect Secrecy. I, a més i si es desitja, amb Clau de Xifrat d'un sol ús ja que en aquesta Criptografia la relació entre les cardinalitats dels conjunts dels Missatges M, dels Criptogrames C i de les Claus de xifrat K és: $Card(C)=Card(M)=Card(K)$.

4. Finalment, hi cal emfasitzar què la "Criptografia" Quàntica (és a dir, la transmissió de la Clau de Xifrat d'un sol ús per al Xifrat de Vernam) només estarà al servei de les institucions econòmicament molt poderoses, mentre que els mètodes de xifrat de la Criptografia Aleph-0 podran ser utilitzats per qualsevol parella d'interlocutors, amb independència del seu poder econòmic.