

Quantum Systems - 1

What type of quantum (non-local) experiment(s) could be tested in space? (Solar system size and beyond)

How much quantum do we actually need for quantum cryptography?
Can we think of a system where a key is transmitted classically (and therefore possibly efficiently) and where quantum states are only used from time to time to check the security of the channel?
Intuition: if two people have to exchange a secret in an isolated room, they don't have to whisper.

Can the decrease in computational (or generic info) resources of a system be related to the emergence of classicality?

Is quantum computation possible with single photons in mixed states (multimodes)?

Why does the cost go up the fewer photons you want to produce?

Quantum Systems - 2

Measurement and the interpretation of quantum mechanics

- Do quantum systems jump without measurement – and which interaction qualifies as a measurement?
 - (i) What is macroscopic (quantitatively) about measurement, i.e., mass, charge, number, etc.
 - (ii) How long do I need to store the information before I can consider it a measurement?
 - (iii) Are (i) and (ii) related, and if so, how?
- Where does the quantum system end – will there ever be an answer more satisfying than the many worlds idea?
- Will there ever be a better interpretation than Copenhagen?
 - *or worse?*
- Shut up and compute?

Complex Systems

Chaotic communication

- How many photons do you need for chaotic communication?
- How does complexity based encryption compare to digital electronic encryption (that runs commercially up to 10 Gb/s)
- What can be an advantage of chaos-based optical crypto with respect to DES or AES since they both rely on computational hypotheses?
- What are the computational assumptions behind chaos based crypto?
- Can you realize (Q)KD with chaotic communication?

Can any cryptosystem be deemed “provably secure” if there are no quantum protocols (as yet) for Alice and Bob authentication?
[woman-in-the-middle attack!]

- Comment – Classical authentication is secure, and it is used in all QKD protocols

Can one benefit from the fundamental unpredictability of chaos?

How far and how accurately can Information Theory describe analogue (real world) coupled nonlinear dynamical systems?

Overlap of Quantum and Complex Systems

The brain

- How is information processing performed in the brain?
- Is our brain encrypting its information (from ourselves)?
- Is brain information encoded/stored/retrieved into “bits”, or rather a “connection pattern”
 - *and is brain information reducible into discrete elements?*
- Is the brain using the most efficient way of information processing?
- What about our BRAIN finally?
 - *particle behaviour, wave behaviour, chaotic system, what???*
- You need more than the brain to understand the brain.

Who will be the first to combine quantum for key distribution and complexity for fast encryption?

Complex systems are everywhere; quantum systems cannot be the exception.

What are the novel chances for information processing?

- What is the price?

Other comments - 1

Quantum info processing:

- what milestones towards a possible revolution

1 – long-lifetime/regenerative qbit?

2 – qbit transport?

3 – practical C-U gates?

4 – massive integrability?

5 – others?

6 – complexity of QKD, no. of operations?

Other Comments - 2

Let us remember

- Normal science = problem solving
according to T. S. Kuhn in “The Structure of Scientific Revolutions”

How does one know if one’s research is following a dead end?

Are there any dead ends?

Real phenomenon = funded phenomenon?

Are funded phenomena necessarily fun?

Are fun phenomena necessarily funded?