

Re: Quantum communication might be possible?

Source: <http://sci.tech--archive.net/Archive/sci.physics.research/2006-01/msg00163.html>

- *From:* Greg Egan <gregegan@xxxxxxxxxxxxxxxx>
 - *Date:* Sun, 22 Jan 2006 22:00:38 +0000 (UTC)
-

In article <dqm70h\$d8t\$1@xxxxxxxxxxxxxxxxxxxxxx>, nmm1@xxxxxxxxxxxxx (Nick Maclaren) wrote:

- > In article <20060118010542.E99924B58A@xxxxxxxxxxxxxxxxxxxxxx>,
> Greg Egan <gregegan@xxxxxxxxxxxxxxxx> wrote:
[snip]
- >> Quantum communication
- >>-----
- >>
- >> Alice and Bob receive sequences of photons which are correlated as above.
- >
- > So this is either an entangled CHANNEL or the number of bits transferred
> is fixed? I am not sure how an entangled channel of photons would
> work, and I was definitely told that the number of bits was indefinite
> (see below).

What I am describing is simply the production and transmission of as many individual pairs of entangled photons as required to fulfill the purpose at hand. The number of bits available is unlimited because the number of photon pairs you can create and distribute is unlimited. This is not the most efficient scheme, but it's conceptually the simplest, so it's worth understanding what's happening here before considering all the various permutations and refinements.

If you want to create and distribute a *single* entangled system, and then use it for applications involving an indefinite number of bits, that's a more complicated matter — and it would always require the parties to keep on sending things to each other; they can't just share a finite entangled system and then expect to communicate an indefinite number of bits, without any further physical exchanges taking place.

For example, there's a sophisticated scheme for quantum key distribution <<http://arxiv.org/abs/quant-ph/9911025>> in which a finite entangled system is created once only, and then two of its qubits (out of a total of six) are repeatedly passed back and forth between Alice and Bob to allow a random key of arbitrary length to be created and shared securely.

- >> Alice and Bob randomly choose between two directions, V and W, which are

Re: Quantum communication might be possible?

- > >45 degrees from each other. After they have collected a large number of
- > >measurements, they publish their choices of directions; this allows them
- > >then to know when they made measurements along the same direction. Their
- > >polarisation results when their directions coincided are known only by
- > >them, and will agree, so they can use this sequence of bits as a secure
- > >key.
- >
- > And it is safe from snooping because, if Cecil does snoop, he will
- > destroy the entanglement and Alice's and Bob's keys will not match.
- > That is a critical characteristic – without it, quantum communication
- > is no advance on distributing two copies of a one-time pad.

Yes, and that's exactly what I'm talking about below. Sorry if I confused you by referring to "statistics about the data"; I was using the word "data" generically, not to refer to a message as distinct from a key.

- > >Any eavesdropper/data-corrupter will not know the choices of direction
- > >made by Alice and Bob, and so will be forced to make his own choices. If
- > >Alice and Bob publish some further statistics about the data, it's
- > >possible for them to verify that no eavesdropping or corruption of the
- > >data has taken place.

The point I was trying to make was, if Alice and Bob end up with different keys because of the intervention of an eavesdropper, how do they establish that fact? They can't publish their entire keys, so it's a matter of judiciously publishing statistics.

- > Eh? At most, that will enable them to say that about the key (and
- > my previous remark addresses that). All of the papers and talks have
- > sworn that snooping on the DATA is also impossible, because at least
- > some of it is transferred by the entangled channel.

Literally dozens of different schemes have been proposed, and what's practical and advantageous will vary from context to context. You can distribute a key by a secure entanglement-based method and then send all the encrypted data classically if you like ... or you can use various quantum methods for everything. The possibilities are endless, but I was trying to outline the most basic version from which the principles can be understood.

The first simple schemes that were envisaged involved the kind of thing I've been discussing -- generating lots of entangled pairs -- whereas more recently people have got excited about various schemes that swap entanglement from one pair of particles to another, an example of "quantum teleportation".

In general, what happens with teleportation is that Alice and Bob first receive particles 1 and 2 which are members of an entangled pair. Alice can then perform a *joint measurement* on the combined state of particles 1 and 3, where 3 is in an unknown state. She then sends the

Re: Quantum communication might be possible?

result of this measurement as 2 bits of classical data to Bob, and he can use it to perform an operation on particle 2 that will put it in exactly the quantum state that particle 3 originally possessed.

This includes the possibility that particle 3 was entangled with some other particle, 4, in which case particle 2 rather than particle 3 will now be entangled with particle 4. Hence we have a case of "entanglement swapping".

My understanding of what's meant by the phrase "entangled channel" in the literature is the ability to take one entangled system and swap the entanglement around from system to system. So rather than just having a specific entangled system, what we have is a certain "amount" of entanglement that we can (at least in principle) shuffle around between different physical systems. This is probably more important for quantum computing than for quantum cryptography.

The crucial point is that an "entangled channel" shouldn't be mistaken for some kind of quantum walkie-talkie that you can pump information through without having other means of communication. If you give Alice and Bob an entangled channel but otherwise isolate them from each other completely, they won't be able to communicate anything.

Greg Egan

Email address (remove name of animal and add standard punctuation):
gregegan netspace zebra net au

.

- *Follow-Ups:*

- ◆ ***Re: Quantum communication might be possible?***

- ◇ *From:* Nick Maclaren

- Prev by Date: ***Re: Fermi's Paradox and DNA***

- Next by Date: ***Re: orbitals, flowers, quantum puzzlement;***

- Previous by thread: ***Re: Quantum communication might be possible?***

- Next by thread: ***Re: Quantum communication might be possible?***

- Index(es):

- ◆ ***Date***

- ◆ ***Thread***