

Re: Crypto Mini-FAQ

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-04/1730.html>

From: Roger Schlafly (*rogersc_at_mindspring.com*)

Date: 04/30/03

Date: Wed, 30 Apr 2003 09:28:21 GMT

"Douglas A. Gwyn" <DAGwyn@null.net> wrote

- > > *Quantum cryptography has nothing to do with quantum computing...*
- > > *Not much, except that quantum cryptography needs a quantum*
- > > *computer in every repeater and router.*
- > *No! Quantum cryptography merely exploits quantum coherence*
- > *to detect intrusion, or meet some other cryptographic goal.*
- > *"Quantum" *equipment* is required, but that equipment does*
- > *not by any means qualify as quantum computing. The two*
- > *really are quite different.*

How do you make a repeater or router without a quantum computer?

- > > *I don't see much difference. Cold fusion and quantum computing are both*
- > > *just ideas. In both cases, the physics says that it might be possible,*
- > *but*
- > > *no*
- > > *one has figured out how to do it. Neither is likely in our lifetimes. If*
- I
- > > *had*
- > > *to bet on one or the other, I am not sure which I would pick.*
- > *Cold fusion was obviously a bogus notion in the first place, ...*

Maybe some breakthrough will make it possible.

- > *Quantum computing, on the other hand, is not only supported*
- > *by theory, but has been reliably demonstrated in the lab*
- > *(although only on a small scale at present).*

I am not convinced of this. There are some quantum mechanics experiments (such as nuclear magnetic resonance) that have been repackaged as quantum computing demos, but I don't think that they have really computed anything, or that they are stepping stones towards building a quantum computer.

There are various people who have claimed to build a qubit, and even someone who has claimed to have factored 15 with qubits, but I don't think that there is even a convincing demo

sci.crypt: Re: Crypto Mini-FAQ

of 1 qubit. I hope they do, but it seems like it will take some sort of breakthrough.