

Re: interesting article on quantum cryptography

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2007-04/msg00789.html>

- *From:* "Douglas A. Gwyn" <DAGwyn@xxxxxxxx>
 - *Date:* Thu, 26 Apr 2007 21:15:07 GMT
-

Antony Clements wrote:

... since according to the article quantum cryptography works with photons, and many of today's encryption schemes use XOR, how would a quantum cryptographic scheme work with such a function. except maybe to compare the intensity of one photon with the intensity of another and the result being the difference in their respective intensities.

There are several issues involved; generally saying "XOR is involved" is pointless, since there are a large number of arithmetic and logical operations involved in implementing the crypto algorithm.

There is "quantum computing" (QC), which should apply to any algorithm, with known advantages over conventional computing (once QC is available on a large scale) in the case of *some* kinds of algorithms. QC could be applied to any crypto algorithm, "XOR-based" or not.

However, "quantum cryptography" (alas, also "QC") usually denotes the exploitation of quantum coherence to implement secure communication channels. The basic principle is that any eavesdropping is detectable by the legitimate communicants. Alternatively, the eavesdropper may only be able to obtain "information" that does him no good with respect to recovering the plaintext or key.

Photons are used in implementations because they are much easier to work with at the quantum-coherence level than any other phenomenon (e.g. electrons).

There is a lot of tutorial information for this field available on line, for example http://en.wikipedia.org/wiki/Quantum_cryptography

.