

The Impact of Quantum Physics on Cryptography Standards

by: Lawrence Bray, 04/25/2005

<http://www.securitydocs.com/library/3230>

Current Computer Systems

Computers are used to process information. In understanding how a computer system is set up we can discover what information would be effectively processed, and what information would be ineffectively processed. The most basic level of a computer system is its *logic gate level*. At this level the computer only knows true or false. This information is carried by the most basic of computer structures, the bit. Ultimately, this is how modern computers process information – through a series of true and false signals carried by bits. Since each bit only contains one true or one false, it takes quite a number of bits to represent any sophisticated information. For instance, to represent a simple letter takes 8 bits.

Current Cryptosystems

Because of the current design of computer systems, some processes are very difficult for a computer to do efficiently. It is precisely these “weaknesses” that current cryptography standards exploit when creating algorithms. Many cryptosystems today use large number factoring as part of their algorithm because it is very difficult for computers to solve such factorings.

Quantum Computing

With the development of quantum physics came quantum computing. Quantum physics has shown that atomic and sub-atomic particles do not necessarily follow the classical laws of physics as larger objects do. Quantum computing suggests that we use this atomic/sub-atomic level to process information in a computer system in place of the bit. One big advantage to quantum computing is that the qubit (quantum bit) is not limited to being set to one state (true or false), but can be both states at the same time. A discussion on the particulars of quantum computing is beyond the scope of this paper, I would recommend [2] for further reading on the subject. The application of a qubit’s ability to be in two states at once has quite an implication with regards to the complexity of problems computer systems would be able to solve. With the qubit a quantum computer would take exponentially less time and memory to process information. Not only will a qubit be able to handle more than one state at once, but also the computer itself will be able to process multiple pieces of information simultaneously (parallel processing) with only one processor. In contrast, current computer systems process information linearly, and one piece at a time; the only way that these computers can perform parallel processing is via multiple processors.

There are, however, some problems facing quantum computing. The number of gates would grow polynomially with the length (in bits) of the number, so the number of trials required would be superexponential [1]. There is also the issue of decoherence, which causes super imposed wave forms to lose their distinctness and makes the computer fail [1]. Today there are designs for quantum computer systems that seek to dissolve these problems. One type of architecture implements the use of trapping ions [4,5]. Trapping ions confines them to a very small space in ultra-high vacuum conditions. In these conditions the ions remain very unpolluted.

Quantum Cryptography

The power that quantum computing can yield is the reason for changing the standard of cryptography. We can’t wait until the computer system is developed to consider its implications. After all, a quantum computer would be able to break any cryptosystem that is based off of large number factoring algorithms (as most cryptosystems are). That means banks, companies, countries, etc. would have no way of keeping information secret.

Peter Shor developed a quantum algorithm (Shor's algorithm) which is able to factor large numbers in polynomial time. His algorithm uses two phases – one for quantum computing, the other for classical mathematic computations. Shor's algorithm brought quantum cryptography to the forefront since being able to efficiently factor large numbers renders most current cryptosystems useless [2].

Today, the general thrust of quantum cryptography usage seems to be in the area of key generation for traditional symmetric encryption algorithms. This application generates the same random number in two locations at the same time. Thus, supplying the key for traditional encryption and decryption techniques. A good resource for further reading on quantum cryptography is [3].

It comforts me to know that as we are working towards producing a quantum computer, we are also advancing in the area of quantum cryptography. While the cryptography is a consequence of the computing, it is of utmost importance that it remain contemporaneous in its development. Otherwise, the gap in advancement may create a security hole - computer systems being created while cryptography standards try to catch up.

References

- [1] Bruce Schneier, "Applied Cryptography", Second Edition, John Wiley & Sons, 1996, page 165.
- [2] P.W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring", in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society Press, Los Alamitos, CA), pages 124-134 (1994).
- [3] Richard J. Hughes, D.M. Alde, P. Dyer, G.G. Luther, G.L. Morgan, and M. Schauer, "Quantum Cryptography" (Los Alamos Technical Report LA-UR-95-806) (1995).
- [4] D. Kielpinski, C. Monroe, D.J. Wineland, "Architecture for a large-scale ion-trap quantum computer" (Nature, Vol. 417), pages 709-711 (2002).
- [5] D. Keilpinski, V. Meyer, M.A. Rowe, C.A. Sackett, W.M. Itano, C. Monroe, D.J. Wineland, "A decoherence-free quantum memory using trapped ions" (Science, Vol. 291), pages 1013-1015 (2001)