Quantum Cryptography Or How To Stay Safe In The Face Of Quantum Computers

Nick Papanikolaou

Quantum cryptography is all about achieving secure key distribution using the phenomena of quantum mechanics. It is now an implemented technology, and promises to work even when large scale quantum computers become widely available. In this article we will try to demystify quantum cryptography. As we will see, quantum cryptography relies on the same fundamental phenomena as a quantum computer, but its security is independent of an attacker’s computational power and so is designed to be safe against such a device. The security of many classical cryptosystems such as RSA, on the other hand, is threatened by the very idea of a quantum computer.

***Note.*** We will use the term ‘classical’ here to refer to computers, algorithms and protocols that are used in traditional computer science; this is in contrast to their quantum counterparts.

# Quantum Computers: Speculation or Reality?

First of all, let’s make one thing clear: quantum computers haven’t yet been implemented on a large scale. To build a large quantum computer is the goal of many an experimental physicist, but while the capabilities of such a device are well understood theoretically, there are many thorny issues that arise in real experiments. A quantum computer consists of *qubits,* or quantum bits, which need to be controlled individually. Qubits arise in nature in the states of atomic-scale particles, such as protons, neutrons, electrons, or even light particles (photons). In particular, a qubit has two distinguished states (usually written |0> and |1>) and an infinity of other possible states, and these states correspond to the values of particular physical properties, such as the angular momentum (or *spin*) of an electron or the polarisation of a photon, at a given moment in time.

To make a quantum computer it is necessary to manipulate qubits individually, in an analogous way to the bits in a classical computer register, which are constantly updated and read by programs. Of course, in the quantum case, states are much harder to manipulate: (i) it is difficult to isolate and control an individual particle from among several, (ii) it is impossible to prevent an individual particle from interacting with its environment. The first issue is because of what is known as quantum *entanglement*. The phenomenon of *decoherence* is the result of (ii), and troubles experimentalists no end. Intuitively one might imagine this as being like noise so prominent that it disturbs our ability to hear and prevents us from understanding a spoken sentence. Combating this noise is very difficult on the atomic scale, and this makes it hard to keep a qubit ‘alive’ and fixed in a chosen quantum state. If the state of a quantum computer is not stable, it is nigh impossible to perform a computation. Developments in experimental physics are expected to make it possible to address these issues on a large scale in the next 10-20 years.

Quantum algorithms are procedures that could be implemented on a quantum computer to solve problems. Some quantum algorithms have been discovered that have significant advantages compared to their classical counterparts, in particular Peter Shor’s factoring algorithm and Lov Grover’s inverse database search algorithm. For example, to factor an integer *N* into a product of two primes, a quantum computer needs on average (log(N))3 steps with Shor’s algorithm, while a classical computer could -at best- do it in a number of steps exponential in *N*. So to factor the number 300000, a quantum computer would only need 75 steps, while a classical computer using the best known algorithm would need 2005 steps! It goes without saying that the ‘steps’ of a quantum computer would each take nanoseconds to execute.

Classical public key cryptosystems such as RSA rely for their security on the difficulty of performing this computation, and in practice use extremely large numbers; being able to perform factoring efficiently makes it easy to break such systems quickly.

For a good, readable introduction to quantum computing consider [Rieffel, Eleanor G. and Polak, Wolfgang. “An Introduction to Quantum Computing for Non-Physicists.” *ACM Computing Surveys 32(3),* pp. 300-335].

# How Quantum Key Distribution Works

Quantum cryptography, or *quantum key distribution* more accurately, allows two parties to establish a common secret (a *key* which can then be used in any private-key cryptosystem, such as the one-time pad) in such a way that an eavesdropper can (i) be detected and (ii) be thwarted. Quantum key distribution is a way of generating a key starting from a random bit sequence; the random sequence is encoded in a stream of qubits which are transmitted over a channel [in practice, this might be photons being transmitted over an optical fibre]. If an enemy tries to intercept the qubits in order to measure them and extract the bit sequence, he or she will inevitably cause a *disturbance* to the qubits that will make the enemy’s presence manifest to the proper users of the channel. They can use some classical protocols (known as *secret-key reconciliation* and *privacy amplification* schemes) to correct errors caused during transmission and eliminate any valid key information that the enemy may have gained in the process.

For an accessible introduction to the detailed workings of quantum key distribution, see [Papanikolaou, Nick. “An Introduction to Quantum Cryptography.” *ACM Crossroads 11.3*, Spring 2004.]

# Limitations and Further Considerations

The security of quantum key distribution lies in two things: (i) the randomness inherent in measuring quantum states (ii) the use of some clever, classical post-processing of the key. Mayers proved that the quantum key distribution protocol BB84 is unconditionally secure against all attacks permitted by quantum mechanics [Mayers, D. “Unconditional security in quantum cryptography.” *Journal of the ACM* **48** (3) (May 2001), pp. 351-406].

Quantum key distribution protocols do not address the problem of authentication: there is no direct way allowing the communicating parties to check they are indeed talking to each other. The proposed solution is to use “Wegman-Carter tags”, but for the security result to be maintained the parties involved need to share some information privately in advance of quantum key distribution. This is a limitation, but for the time being it does not seem to be a substantial impediment for practical applications.

The key point to remember is that quantum key distribution does not rely for its security on the difficulty of any computational problem; its security is provided by fundamental properties of nature as we understand it, specifically the way quantum measurement works.

For business applications, quantum cryptography is not a substitute for PKI – while PKI may be threatened if large scale quantum computers materialise, to use quantum cryptography would mean generating new keys for every business transaction or communication. How quantum cryptography can be deployed for such applications is an interesting question.

**Nick Papanikolaou**