

Quantum Cryptography: Uncrackable Codes?

Michael Turner

From the mysterious world of cutting edge modern physics, quantum cryptography could soon become a multi-billion dollar industry. Society is increasingly dependent on computer systems, and communicating information securely is vital. Current systems—such as the RSA cypher—owe their security to the limits on available computing power. Quantum cryptography has the potential to revolutionise personal data security, and decide once and for all the battle between code makers and code breakers that has raged for over 2000 years. Everything from personal banking data to national intelligence flies

system stands to make a fortune.

In the language of cryptography, encryption systems allow a sender, 'Alice', and a receiver, 'Bob', to communicate a message that is scrambled using a key.

The first quantum cryptosystems are in fact already here

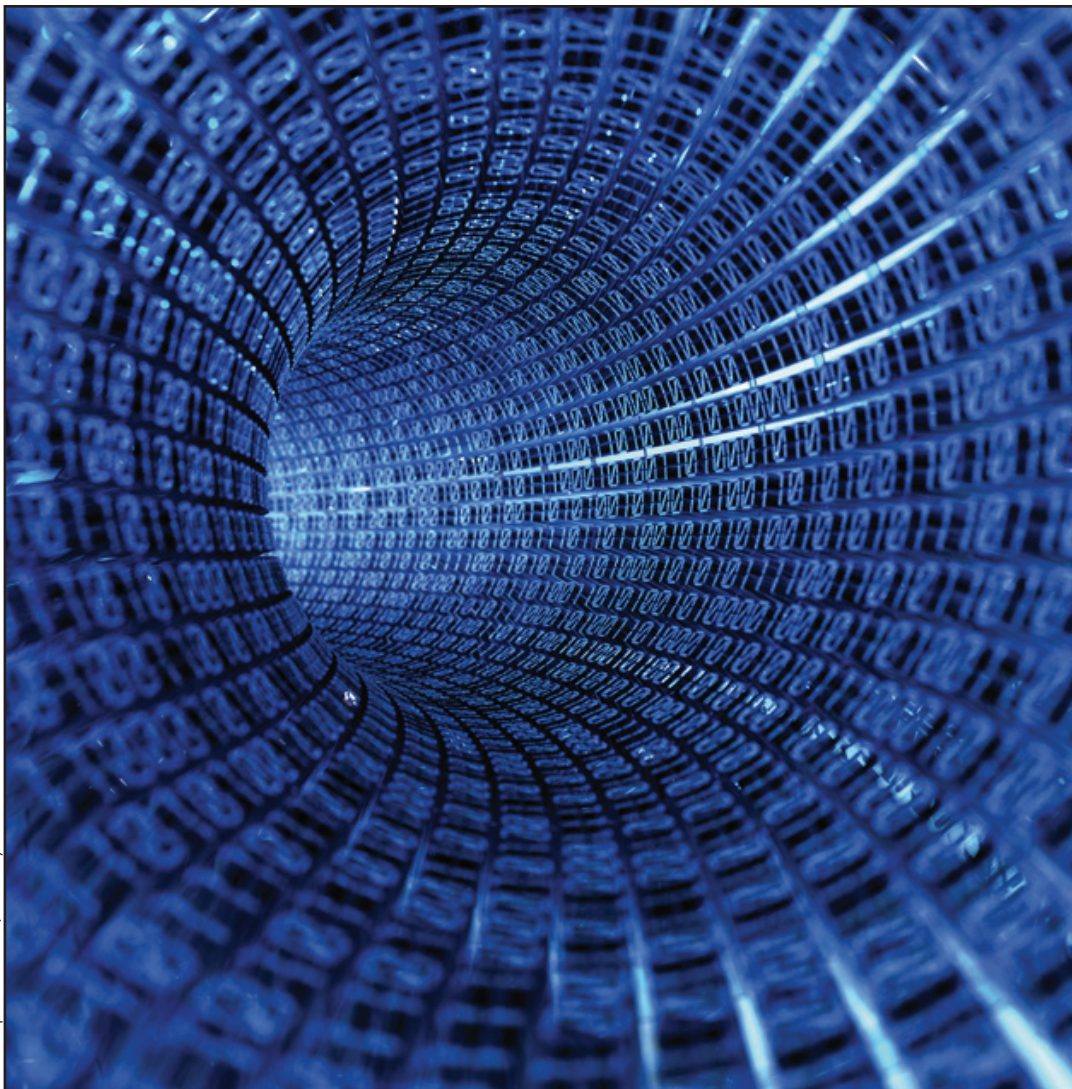
across the internet, so the person who develops the first fully implementable and affordable quantum-based security

Quantum cryptography has the potential to revolutionise personal data security

Problems arise in the difficulty of Alice getting this key to Bob without an eavesdropper, 'Eve', getting her hands on it too. The RSA cipher, one of the main cyphers used today, uses a 'one-way function' to encrypt the message. Alice first looks up Bob's 'public key', which is freely available, and uses it to encrypt her message. The public key is a number generated by multiplying two very large prime numbers—the message

can only be deciphered by someone who knows these numbers, called Bob's 'secret key'. Eve can intercept the message undetected, but does not have the secret key to decode it. She must find the two prime factors of the public key. Although modern computers would take too long to do this calculation usefully (1), a future quantum computer would have such awesome power that breaking today's best encryption would be child's play. It is ironic, then, that quantum physics also holds the prospect of finally creating a perfectly secure means of communication: quantum cryptography.

The first quantum cryptosystems are in fact already here: the two leading companies, ID Quantique SA in Geneva (2) and MagiQ Technologies Inc. in New York (3), already sell systems for \$100,000 apiece (4). An ID Quantique system was used to safeguard last year's Swiss election



©iStockphoto.com/Andrey Prokhorov

against corruption or malicious tampering (5). The consequences of quantum cryptography becoming widely available are far-reaching. Governments would be unable to breach the private communications of citizens, but neither could they intercept the dealings of criminals and terrorists, who would be free to organise themselves in almost perfect secrecy. On the one hand, it is a fundamental right that "no one shall be subject to arbitrary interference with his privacy" (6). On the other, there is the need for security in an increasingly unstable world; it is a sad fact that organised crime rings would be some of the 'businesses' in the best financial position to implement such systems when they become available (7).

Many governments already have legislation in place to overcome some of the barriers created by current cryptographic systems. For example, the UK Regulation of Investigatory Powers Act (2000) allows for "lawful interception", effectively forcing anyone subject to enquiry to provide either the required unencrypted information or the encryption key (8). Similar legislation in the US, the Senate Bill 266, requiring every piece of cryptographic

Criminals and terrorists... would be free to organise themselves in almost perfect secrecy

software to have a built-in back door, was defeated in 1991 after strong protests from civil liberties groups (9, 7). In fact, some current encryption software packages come complete with built-in backdoors, and would-be terrorists have been caught by such features (1). With quantum cryptosystems, however, governments could only retain their interception abilities by restricting the flow of such technologies into the marketplace.

Enforcing any way to get around an 'unbreakable' system would somewhat negate the impact of having such technology. If governments were to implement tight restrictions on the use of quantum cryptography, law-abiding citizens could still be subject to interception of their private messages. However, those with the necessary resources and a desire for complete security could merely employ the system to its full potential, even in the face of the law.

Despite direct eavesdropping being impossible, quantum cryptography could still succumb to other types of attack. Eve could impersonate both Alice and Bob and act as a man-in-the-middle, persuading Alice to tell her the

Some current encryption software packages come complete with built-in backdoors

message, then re-encrypting it and sending it on to Bob. To counter this, there are systems of authentication, but these rely on sharing some secret knowledge beforehand, via less secure routes. A quantum cryptosystem would also be vulnerable to communication disruption, in which Eve

repeatedly interferes with the line so that the message cannot be sent, causing great problems for the sender (7). Future technological advances may also allow photons to be stored in a trap for relatively long periods of time. Eve could use this to split the beam, effectively copying the string of photons without altering them, and then storing this copy until Alice and Bob agree on which bits to use and how to measure them (7).

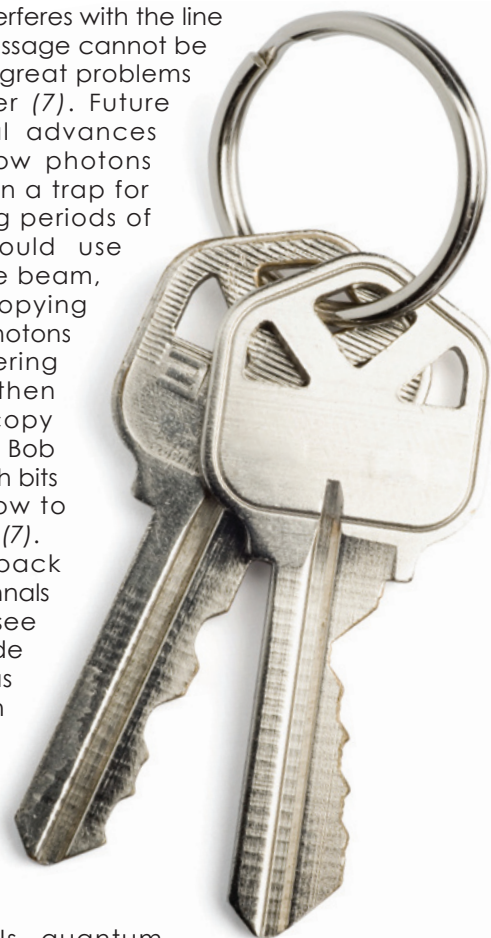
Looking back through the annals of history we see that every code and cipher has been broken eventually; the RSA cipher needs only the advent of the quantum computer to become

vulnerable. Is quantum cryptography only a step away from being breakable as well? If beam splitting and photon traps develop into feasible and effective methods of interception, then the situation may not be much different from today; someone with enough resources and technology could again intercept private messages without being detected. Will quantum cryptography one day go down in the annals alongside Le Chiffre Indéchiffrable and Enigma, codes their users once thought to be unbreakable? Only time will tell...

Michael Turner is a 2nd year reading Physical Natural Sciences at St John's College.

References:

1. Singh, S. *The Code Book*; HarperCollins, London, 1999.
2. ID Quantique, www.idquantique.com
3. MagiQ Technologies, www.magiqttech.com
4. ITWorldCanada.com **2007** www.itworldcanada.com/V.aspx?i=77d83ee975194f63828b
5. New Scientist **2007** technology.newscientist.com/channel/tech/dn12786-quantum-cryptography-to-protect-swiss-election.html
6. United Nations Universal Declaration of Human Rights, Article 12 www.un.org/Overview/rights.html
7. Next Generation Security Software **2003** www.ngsconsulting.com/papers/quantum_cryptography.pdf
8. Regulation of Investigatory Powers Act 2000, Chapter 23 www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm
9. Comprehensive Counter-Terrorism Act of 1991 (Senate Bill 266), Section 2201.



©istockphoto.com/bluestocking