

Quotations

Quantum Cryptography is a hacker's nightmare but a dream for bankers: a computer network so secure that even the simplest attempts to eavesdrop will alert administrators to the snooping.

Associated Press. Cambridge Mass. Sep 04.

It is important the financial community should be made aware of the implications and state of play of the development of quantum cryptography.

Alastair Clark , Bank of England.

The City of London generates a substantial portion of the GDP of the UK. Its business and reputation relies to a considerable extent on its reputation for security. Given the potential risks of a breach of this security, and the damage that even rumours that this security might be vulnerable could cause, it would seem prudent to invest a modest number of millions of pounds to take some cautious steps to insure against such an eventuality.

Professor Brian Collins

We have our hands full trying to ensure our members follow even rudimentary procedures to maintain simple levels of security. We really do not have time to worry about the whole system collapsing.

Unattributable

We have a queue of people offering us 'unbreakable' key systems. We have no difficulty distributing keys. We have little interest, therefore, in a 'quantum key distribution system'.

APACS

Many people have no idea how existing cryptography works. They do not have the means to measure the risk of this technology being compromised. They have even less understanding of quantum cryptography and therefore no idea of its potential benefits.

Andrew Hilton CSFI

The cryptographic community have to be prepared for the possibility of a breakthrough in prime numbers that might give insights into factorization. If you ask my opinion, I think any such breakthrough is very unlikely. It is more likely that someone will be able to prove that factorization is a hard problem. But if you'd asked me in the mid eighties whether I thought Fermat's Last Theorem would be proved in the next ten years I would also have said "unlikely".

Marcus du Sautoy. Professor of Mathematics Oxford University

The most effective way of breaking into a communication system is simply to disrupt the system, then when the target moves to a back-up system, which is usually the previous technology, break in to that.

GCHQ

Questions and Comments at the Meeting of industry leaders at the Department of Trade and Industry Sep 3rd 2004

Is the ability of your system to identify an eavesdropper absolute, or a matter of statistical analysis?

If you are using line of sight systems would the state of the weather interfere with communications?

If this technology relies on identifying the mere presence of an eavesdropper, then could the communication link be effectively put out of action simply by eavesdropping and therefore denying service?

The DTI can play its part in stimulating the development of new technologies, but industry must also contribute.

QC really is futuristic technology. Its applications are going to be a lot like the laser and the transistor, in that early people could not think of all the possible applications and uses of it.

John M Myers: Harvard

QC is like computing all over again. We cannot possibly tell what the implications may be.

Andrew Hilton CSFI

We estimate the potential market for Quantum Cryptography is likely to reach \$1 billion per annum.

Bob Gelfond. MagiQ Corporation. New York

The most difficult phase for any new technology is when the inventors are not clear how the potential customers might use it, and the potential customers do not understand what is being offered.

Venture Capital Conference

It is reasonably certain that if we rely on the provision of venture capital to develop quantum computing in the UK, then this technology will be implemented overseas and the UK, having contributed substantially to its invention, will end up importing it: a repeat of the history of the computing industry. The private company BBN Inc in the USA has a substantial, well published contract to develop applications from DARPA. One other commercial supplier is known to have received a major contract from a defence source. Venture capitalists will not invest their funds to compete against governments. Many people working in Quantum Information Processing abroad are ex-pats.

Real Time Club

The only thing we know for certain is that we know nothing for certain.

Socrates

Constructive Uncertainty.

A quantum version of Socrates' quotation.