

Awareness of Market Failure Issues

1. Market Failure

Market failure, or the inability of normal commerce to develop a timely market, occurs for a variety of reasons but is particularly prevalent in the application of new and novel technologies. Quantum cryptography appears to be no different.

2. Understanding

Quantum physics, and in turn quantum cryptography, is a difficult science with curious attributes and confusing concepts. It diverges significantly from, and in some areas conflicts, with conventional physics. For some people this takes it into the realms of science fiction.

For a few business executives this is exciting and worthy of interest, for some it is too difficult and confusing, but for many it is a closed book and readily ignored. Levels of knowledge and interest in the business community are low. As one executive commented, “This isn’t rocket science – it is much more difficult than that”.

The lack of understanding goes further and even in the scientific community there is a failure to embrace quantum. As the Report of the Quantum Cryptography Technology Experts Panel (July 2004) claims “Potential practical uses of QC are relatively unexplored owing to the inaccessibility of the technology to the conventional information assurance and communications research communities”.

Even project teams working on similar projects have exhibited disagreement over what were assumed to be widely accepted facts.

3. Information

The quantum science communities have communications mechanisms – websites, conferences, seminars – to maintain a flow of information amongst themselves. This does not however translate into information for the business community in a format which is accessible and relevant. There are many examples of misunderstandings about the state of the art and of its

capabilities. This is all compounded by the rapid progress in development and the absence of any communication mechanism targeted at potential customers and users. Raising awareness amongst appropriate constituencies in an objective and balanced way is important and becoming urgent.

4. Requirements

There is an observable chasm between the teams developing “product” and the potential user community. Not only do the developers have an opaque view of market needs, the potential customers have done little or nothing to determine requirements.

This project has already brought “suppliers” and “customers” together with beneficial results. But this is only scratching the surface and much more needs to be done in a sustained and objective way to encourage and facilitate a continuous dialogue.

5. Reporting

Media reporting of developments, innovations and applications will have a significant impact on the understanding and acceptance of QC. As with other communities there is concern about misunderstanding and/or misinterpretation. With the ability of the media to over-simplify and sensationalise, the risks of mis-reporting are significant even if the understanding of the technology and its implications is sound.

A recent example illustrates the point. At a British Association conference (September 2004) a claim was made that a proof had been discovered for Reimann’s Hypothesis (which concerns patterns in prime numbers) and this might have implications for cracking current coding systems. It is unlikely the proof is valid and, even if it were, there are no direct or immediate implications for breaking classical cryptographic codes. Nevertheless the press reported the story and commented:

“If true the solution could undermine Internet Security”. (eCommerceTimes)

“Proof of the hypothesis would mean all cryptic codes could be breakable, so no Internet transaction would be safe”. (finextra.com)

“Maths holy grail could bring disaster for internet”. (Guardian)

The fact is that, unlikely as it may be, if a mathematician does come up with a clever way to factorise large numbers quickly and easily, then the whole cryptography system would be compromised, and there is no defence in place to counter such an eventuality. To avoid misleading stories and sensationalism a media briefing programme for select influential journalists will be required as well as a ready source of sound, balanced information expressed in straight forward terms.

6. Market Collapse.

A significant problem associated with preparing to meet the quantum challenge, or just to keep abreast of communications developments, is that no one organisation is responsible in any one country. While individual institutions have embraced information technology, there is no focal point and no one organisation which has a vested interest, or responsibility for the general security of the national and international traffic over the communications networks. The recent move to chip and pin has come about by the co-operation of financial institutions as a response to increasingly severe losses due to the weak security of the previous payments system.

Unless a similar co-ordinated move can be encouraged it is possible that no avoiding action will be taken and that quite suddenly entire commercial communications networks could be compromised.

Loss of confidence alone caused by perceived threats to reputation and trust could be sufficient to trigger alarm and cause severe damage to ecommerce.

7. Standards and Protocols

New networks, technologies and applications will impact business processes, require interoperability and need to be scalable. For orderly and effective implementations a raft of standards, protocols and agreements will be required. Whilst defining absolute standards too early can be unnecessarily constraining to the deployment of effective solutions it is also the case that market growth and applications development can be severely handicapped by a lack of common standards. No evidence has been found of even preliminary consideration of such issues.

8. Conclusion

Market development will be retarded unless these issues are addressed and market failure is a distinct possibility.