

Market Drivers

1. Threats

Classical cryptography systems are well-understood, relatively safe and, despite the issues with key distribution, cost effective. Key systems are also eminently scalable and there is little concern that improvements in the performance of conventional digital computing will compromise them.

All key systems depend on the inability, in any reasonable time, to factor large numbers. If fast factorisation becomes a reality current secure systems become vulnerable. There are two ways in which this might happen. Quantum computers will be able to factor numbers of any size speedily and simply. Such technology may be some way off but, as this report demonstrates, there is significant investment and activity at a host of academic and research institutions. All the experts contacted believe that quantum computers will become a reality and hence classical cryptographic systems will be at risk. As Baroness Professor Susan Greenfield, President of the Royal Institution said, “We shouldn’t be so smug as to assume that quantum computing will not be practical for many years to come”.

The other risk to classical systems is the discovery of a fast factorisation algorithm. Mathematicians are known to be working on such solutions but if and when the breakthrough will occur is impossible to predict. In the worst case scenario an algorithm might be discovered in the near future which would compromise secure transmissions. If such a discovery were kept secret the consequences would be even more catastrophic.

Visa International describes the commercial need as follows. “Business, especially the financial services industry, relies upon the ability to keep its secrets secret. Compromise of information security is the basis for financial fraud and can undermine confidence; the rise of asymmetric terrorist threats increases the danger that an attack on financial and business systems could be designed with the latter effect in mind and the intent to cause economic disruption.

Secure transmission of data is a key element in information security, but at present creates twin headaches:

- perpetual updating of codes on millions of machines, every time a key is broken, compromised or assessed to be at risk;
- the danger that a code is not updated fast enough; that advances in breaking codes are not anticipated sufficiently quickly to replace existing security before an attack is made.

The major criminal organisations responsible for most financial fraud and certain amongst the plethora of terror groups are well funded and have access to highly skilled computer experts. At the extreme level, there is the (hopefully distant) risk that one amongst them will break the fundamental basis of public key cryptography – the difficulty in factoring large prime numbers. This threat arises primarily from advances in mathematical techniques (whilst quantum computers would shoot a silver bullet at the problem; an apt algorithm represents a much closer risk). Before that point is reached the difficulty comes in estimating when a particular code – or the whole system – will be compromised and taking action in time. Waiting to start work on an alternative until the current approach is known to be redundant would guarantee that at that moment all secure systems would immediately become prone to compromise.

Quantum cryptography offers a completely secure path for the transfer of information: it does not guarantee there will be no failures at other points – that decrypted data will not be mismanaged nor that a trusted individual will turn out to be a fraudster – but it does remove any question about the security of data transmission, and in doing so not only rules out certain forms of criminal attack, but also frees firms to concentrate on improving security in areas where risks remain”.

Marcus du Sautoy, Professor of Mathematics Oxford University commented recently that “ 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"”.

There is a further less well defined but equally important threat. The whole commercial infrastructure, and particularly financial services, depends on reputation and trust. These attributes have been carefully husbanded over many years and, although not directly quantifiable on the balance sheet, are intrinsic to and inseparable from successful commerce – both business-to-business and business-to-consumer. Similar considerations also apply to government communications. Whereas trust and reputation take a long time to generate and much effort to sustain they can be rapidly compromised.

The direct threat is that the commercial infrastructure could be severely damaged by the loss of trust and reputation caused by the belief that it had been, or was likely to be, compromised. This could happen at any time and, if fanned by ill-informed or sensationalist reporting, could have significant and long lasting impacts.

2. Opportunities

QC has attributes that could offer advantages over classical systems. QC systems are provably secure and obviate the need for distributing, storing and managing physical keys. This reduces costs, and removes complex logistical options and renders systems less likely to compromise.

Uniquely, QC also offers the benefit of assured notification to the sender of any attempt to interrupt or eavesdrop on a message.

This latter attribute of QC systems may, when QC systems are robust, be sufficient to justify investment for specific applications.

3. Summary of Risk

The following table of risk, timescale and effect related to secure communications is relevant to all market sectors, although to varying degrees.

Risk Identification	Likelihood	Timescale	Effect	Mitigation
The development of progressively	Certain	Continuous development in line with	Nil, as classical cryptographic	No action

more powerful digital computers		Moore's Law	systems will remain competitive	
Quantum computing	Certain	Indeterminate	Catastrophic as quantum will be impervious to complexity	Monitor developments and develop counter measures
Mathematicians and hackers	Possible	At any time	Might be clandestine and therefore might undermine commercial markets and currencies	Broaden knowledge of alternatives through pilot schemes
Standards and protocols established elsewhere	Probable	Imminent	Loss of control	Take leadership role in standards setting

4. Market Drivers by Sector

Current limitations of QC restrict its potential use to point-to-point systems. The table below considers market drivers by sector based on commercial products (when available) with these limitations. As QC develops as a networked solution the market opportunities will be greatly enhanced.

Audience/Sector	Opportunity	Threat
Commercial/Industrial	Commercial applications of QC are unlikely to impact the vast majority of business until QC is networked, economic and working to	Current cryptographic systems are broken rendering e-commerce unviable

	standards	
Intra Government and Defence	Inter departmental communication can be assured that no-one has eavesdropped on messaging reducing leaks and enhancing communication auditing	Leaks and communication interception on very sensitive information
Financial Institutions	To develop systems that enable institutions to know if communications have been eavesdropped and react appropriately. The opportunity to develop highly secure systems between locations with an absolute need for the best security. QC offers an alternative back-up system	Current security systems become compromised through attack.
Credit and payment systems	Payments systems have a low opportunity from QC as the bulk of their transactions are relatively small and therefore losses are tolerated over costs of implementing and managing new technology	If, however, fast factorising of prime numbers became widespread, then the risk of criminal attacks on the system could be pandemic
General Public	The general public has no immediate need for QC, however, security from viruses and e-commerce fraud are	

	<p>undermining public confidence in the Internet. Therefore, security and cryptography are of genuine interest to the public at large especially the social implications of secure private communication.</p>	
--	---	--