Beating the dark side of quantum computing

November 16 2012

A future quantum computer will be able to carry out calculations billions of times faster than even today's most powerful machines by exploit the fact that the tiniest particles, molecules, atoms and subatomic particles can exist in more than one state simultaneously. Scientists and engineers are looking forward to working with such high-power machines but so too are cyber-criminals who will be able to exploit this power in cracking passwords and decrypting secret messages much faster than they can now.

Now, Richard Overill of the Department of Informatics at King's College London is working in the field of digital forensics to develop the necessary tools to pre-empt the cyber-criminals as quantum computing becomes reality. Writing in the *Int. J. Information Technology, Communications and Convergence*, Overill explains that while quantum computing is in its infancy, as with earlier technological leaps once the nuts and bolts are in place, it will be adopted rapidly by computer scientists and others eager to utilise its enormous potential.

The technologies that will underpin quantum computing will be quite esoteric to the non-specialist and include laser-excited atomic ion traps using beryllium or calcium atoms, bulk liquid-phase and solid-phase nuclear magnetic resonance, as well superconducting solid-state circuits operating at liquid helium temperatures. Of course, the semiconductor, silicon chip technology underpinning current supercomputers is perhaps just as esoteric although seems more familiar to us now.

Nevertheless, it is not the complexities of the technology that is

important but what it will allow computer users to do such as solving logistics problems by overlaying all possible solutions and allowing quantum mechanics to find the optimal route, for instance. Or creating encryption keys that could never be cracked by a conventional computer. And, as Overill warns, providing those intent on cracking passwords and such to apply computational brute force with immeasurable efficiency. Such power might be wielded by crime fighters and criminals alike.

"At first sight, therefore, it would appear that with the advent of practical quantum computers the task of cyber-law enforcement will become significantly more challenging," says Overill. However, as has always been the case with crime and crime fighting, forensics constantly plays catch up with the technology exploited by criminals and so too with quantum computers. Overill provides a roadmap for how research into digital forensics must progress if crime fighters and investigators are to keep up with the pace of change.

Currently there is no answer to beating quantum crime. "There are ultimate physical limitations on what forensic information can be recovered from a quantum computation," says Overill. Forensic has always had such limitations but investigators are adept at obtaining clues regardless. "So, our digital quantum forensics mission has to focus on learning how to get 'more from less', by squeezing every last drop of information from the traces that can be recovered, and then devising novel techniques to interpret these traces as richly as possible."

More information: Overill, R. Digital quantum forensics: future challenges and prospects. *Int. J. Information Technology, Communications and Convergence*, 2012, 2, 205-211.

Provided by Inderscience Publishers