Digital Quantum Forensics: Challenges and Responses

Chapter · January 2011

DOI: 10.1007/978-3-642-22309-9_13

1 author:

Richard Overill
King's College London
120 PUBLICATIONS **1,536** CITATIONS

SEE PROFILE

Digital Quantum Forensics: Challenges and Responses

Richard E Overill[1]

[1]Department of Informatics, King's College London, Strand, London WC2R 2LS, UK

richard.overill@kcl.ac.uk

Abstract. Recent developments in technology suggest that within the next one to two decades some form(s) of quantum computing device will become viable. Once such devices become generally available they will doubtless be employed by cyber-criminals to perform brute-force decryption tasks that were previously infeasible. This paper attempts to address the question of how digital forensic investigation techniques will need to develop in order to respond to the challenges posed by such future generation computing devices.

Keywords: quantum computation; digital forensics; quantum forensics**.**

1 Introduction and Background

The current state-of-the-art in quantum computing suggests that, despite much theoretical and experimental work over the past 25 years, the topic is still in its infancy, both as regards the technologies in which it can be implemented and also the range of algorithms available.

Current candidate technologies include laser-excited atomic ion traps using beryllium or calcium atoms, bulk liquid-phase and solid-phase nuclear magnetic resonance (NMR), and superconducting solid-state circuits operating at liquid helium temperatures (*circa* 4 degrees Kelvin). To date the maximum number of participating quantum bits (qubits) that has been reached is 12 [1], which in principle enables problems of size $2^{12} = 4096$ to be addressed.

The currently available algorithms for quantum computers include Shor's $O(n^3)$ integer factorization and discrete logarithm [2, 3], which could be employed cryptanalytically to attack both RSA-like and EC-based public-key cryptosystems, and Grover's $O(\sqrt{n})$ search algorithm [4, 5], which could be used in an exhaustive search of the key-space of a conventional symmetric cryptosystem such as AES. Due to the intrinsic nature of quantum computation, as outlined in the following section, these quantum algorithms will be capable of compromising many state-of-the art cryptosystems in a matter of minutes or even seconds of real-time. For example, Shor's algorithm could be used to factor numbers100 decimal digits long in a fraction of a second. Quantum speed-up inevitably means that cryptographic cover times which were previously unbreachable cannot be expected to remain intact in the future. In the context of anticipating future large-scale cyber-crimes executed with the aid of

quantum computers, this paper aims to address the key issues of the quality and the quantity of digital forensic evidence that may be recoverable from these devices, and also to indicate how such evidence may be analyzed and interpreted for subsequent forensic use in judicial proceedings.

2 Quantum Computation

Quantum computation [6] exploits the evolution in Hilbert space of a coherent linear superposition of quantum states such that each component of the superposition follows a distinct computational path. A final decohering operational step, which is equivalent to performing a measurement or an observation, then extracts the required output with high probability. Whereas in classical computing a bit is a binary digit which has a value which is either zero or one, in quantum computing a single qubit can in general be an unequal linear superposition (or 'mixture') of the basis states zero and one:

$$|\Psi> = \alpha|1> + \beta|0>, \text{ where } \alpha^2 + \beta^2 = 1$$

From an *n*-particle quantum system an *n*-qubit register (qureg) may be constructed:

$$|\Psi_n> = |1> \otimes |1> \otimes \ldots \otimes |1> \equiv |11 \ldots 1>$$

Applying to this qureg a Walsh-Hadamard transformation, represented by a unitary operator U_H which transforms a single basis eigenstate into an equal superposition of the two basis eigenstates, generates a coherent equal superposition of all 2^n possible inputs:

$$\begin{aligned} |\Psi_n>' &= U_H \otimes U_H \otimes \ldots \otimes U_H \, |11 \ldots 1> \\ &= \left(1/\sqrt{2^n}\right) \times (|1> + |0>) \otimes (|1> + |0>) \otimes \ldots \otimes (|1> + |0>) \\ &= \left(1/\sqrt{2^n}\right) \times (|11 \ldots 1> + |11 \ldots 0> + \ldots + |00 \ldots 0>) \end{aligned}$$

Note that applying a linear (*n*-1) number of operations to the qureg yields a register state which is a superposition of an exponential (2^n) number of terms. This exponential performance is one crucial characteristic of the potential power of quantum computation which distinguishes it from other unconventional computational models, such as DNA computation, swarm computation or evolutionary computation, that scale linearly with *N*, the number of molecules, particles or entities in the system [7].

The prepared register state is input into a quantum logic network constructed from quantum logic gates. Two important kinds of gate are the one-qubit unitary gates, such as the Hadamard, Pauli, and phase-shift gates, and the two-qubit controlled-unitary gates, such as the controlled-NOT (C-NOT) gate. The quantum logic network is designed to carry out a specific quantum computation by unitarily evolving the

input state into the output state, which is a coherent linear superposition of all the possible outputs from that computation. It is then necessary to extract the single required component from the output state, and this is generally achieved by means of a process, referred to as controlled decoherence, that repeatedly enhances the amplitude of this component at the expense of all of the remaining components' amplitudes. It is then highly probable (although not absolutely certain) that an observation or measurement of this state will yield the required component.

Note that it is not fruitful to attempt to directly observe the superposed output state prior to controlled decoherence since the act of measurement will cause the state to decohere spontaneously (or 'collapse') to a single randomly selected component with a consequential loss of information. Note also that as a consequence of the no-cloning theorem [8, 9] it is not possible to clone an exact copy of an arbitrary unknown quantum state for preservation and subsequent analysis, although approximate copies of quantum states can be made.

3 Quantum Forensics

The topic of quantum forensics has so far received virtually no consideration from researchers [10]. In order to understand the possibilities for digital forensic examination and analysis of quantum computers, it is convenient to employ the conventional division into *in vivo* (live) forensics and *post mortem* forensics. From what has already been said above it will be clear that it is not possible to perform live system forensics on a quantum computer, since any observation or measurement made on an evolving superposed state will cause it to collapse to a single randomly selected component. At that instant the states of the system and the observer or measuring apparatus in their environment become correlated (or 'entangled') and useful state information leaks from the system into the composite super-system from which it cannot be recovered.

At first sight, *post mortem* forensics offers a somewhat more encouraging prospect. After the termination of a quantum algorithm and the recovery of an output state generated by controlled decoherence, a single classical output may remain for conventional digital forensic recovery and analysis. Of course, conventional anti-forensics techniques may be used to remove this trace. However, since there is no possibility of observing the intermediate (non-classical) states of the quantum computer *post mortem*, it will not be possible to reconstruct a timeline for the evolution of the quantum computation. This restriction places quite severe limitations on both the quantity and the quality of the evidential traces that may ultimately be recoverable. Since the probative value of digital evidence depends to a considerable extent upon the contextual support it receives from ancillary evidence, it would appear to be very difficult to build a judicially convincing case from the available digital forensic evidence alone.

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. Not only will quantum cyber-criminals be able to gain access to devices capable of breaking a variety of both symmetric and asymmetric state-of-the-art cryptosystems well within any realistic cover time, but their activities will also leave behind a minimal set of recoverable forensic traces for use in any subsequent prosecution. It is this doubly challenging prospect that has given rise to the present study.

A road-map for future digital forensic investigations of quantum cyber-crimes should therefore focus attention on the maximum amount of information that can be elicited from the recoverable evidence, which could potentially amount to just a single trace. If it could be demonstrated with high probability that the *only* feasible route leading to the creation of a single recovered evidential trace necessarily involved the unauthorized perpetration of the cryptanalytic process as alleged by the prosecution, then it might indeed be possible to mount a plausible judicial case.

In fact, recent research in this area, using the actual data from real-world criminal cases involving peer-to-peer file-sharing [11] and online auction fraud [12] respectively, has demonstrated that the application of computational complexity theory [13] and the Keystroke-Level Model (KLM) [14] within the framework of an Operational Complexity Model (OCM) [15], together with the use of Bayesian inference networks for reasoning about digital evidence [11, 12], does indeed offer a realistic prospect of quantifying the posterior odds and the likelihood ratios of competing hypotheses concerning the feasible routes leading to the formation of the recovered digital evidential traces [16]. In particular, by enumerating and analyzing all feasible routes j by which the recovered evidential traces could have been produced, the likelihood ratio of feasible route i is given by:

$$\Lambda_i = \Pr(E|H_i) \,/\, \Sigma_{j \neq i} \Pr(E|H_j)$$

and the posterior odds of feasible route i is given by:

$$O_i = \Pr(H_i|E) \,/\, \Sigma_{j \neq i} \Pr(H_j|E)$$

where $\Pr(E|H_i)$ is the probability that evidential trace E is found given that the hypothesis that feasible route i was taken is correct, and $\Pr(H_i|E)$ is the probability that the hypothesis that feasible route i was taken is correct given that evidential trace E was found.

4 Summary and Conclusions

We have examined how the operation of a quantum computer in the hands of cyber-criminals attempting to break a state-of-the-art public-key or private-key cipher may result in the creation and recovery of one or more digital forensic evidential traces.

However, very the nature of the quantum computational process precludes the creation and recovery of any useful information concerning the intermediate states in the evolution of the quantum computation. Furthermore, it also precludes the possibility of live forensics *per se*. It is probable that the lack of this ancillary evidence will prove to be a significant barrier to mounting successful judicial prosecutions in cases of serious quantum cyber-crime. However, recent and ongoing developments in quantifying the probative value of digital forensic evidence may be able to offer at least a partial resolution of this problem. Further detailed research in this area would therefore be well motivated and of great potential value.

References

1. Reich, E.S., Quantum Computers Move a Step Closer, Nature, 467, p.513 (30 September 2010).

2. Shor, P.W., Algorithms for Quantum Computation: Discrete Logarithms and Factoring, Proc. 35th Annual Symposium on Foundations of Computer Science, IEEE Press, pp.124—134, (November 1994), quant-ph/9508027.

3. Shor, P.W., Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. Comput. 26, 1484—1509 (1997)

4. Grover, L.K., A Fast Quantum Mechanical Algorithm for Database Search, Proc. 28th Annual ACM Symposium on the Theory of Computing, pp.212—219 (May 1996), quant-ph/9605043.

5. Grover, L.K., Quantum Mechanics helps in Searching for a Needle in a Haystack, Phys. Rev. Letters 79, 325—328 (1997)

6. Mermin, N.D., Quantum Computer Science: an Introduction, Cambridge, UK, Cambridge University Press (2007)

7. Overill, R.E., Parallelism of Paradigms in Non-Classical Computation, in Proc. Intl. Workshop: The Grand Challenge in Non-Classical Computation, Ed. Stepney, S., York, UK (April 2005)

8. Wootters, W.K., Zurek, W.H., A Single Quantum Cannot be Cloned, Nature, 299, 802—803 (1982)

9. Dieks, D., Communication by EPR devices. Physics Letters A, 92 (6), 271—272 (1982)

10. Konstadopoulou, A., From Quantum Security to Quantum Forensics, Proc. 1st Conference on Advances in Computer Security and Forensics (ACSF), Liverpool, UK, pp.105—111 (July 2006)

11. Kwan, M., Chow, K-P, Law, F., Lai, P., Reasoning about Evidence using Bayesian Networks, Proc.4th Annual IFIP WG 11.9 International Conference on Digital

Forensics, Kyoto, Japan (January 2008), Advances in Digital Forensics IV, Ch.12, pp.141–155, Springer (2008)

12. Kwan, Y.K., Overill, R.E., Chow, K-P, Silomon, J.A.M., Tse, H., Law, Y.W., Lai, K.Y., Evaluation of Evidence in Internet Auction Fraud Investigations, Proc.6th Annual IFIP WG 11.9 International Conference on Digital Forensics, Hong Kong (January 2010), Advances in Digital Forensics VI, Ch.7, pp.95–106, Springer (2010)

13. Papadimitriou, C.H., Computational Complexity, Addison-Wesley, Reading, MA (1994)

14. Kieras, D., Using the Keystroke-Level Model to Estimate Execution Times, University of Michigan (2001), available online at: http://www.cs.loyola.edu/~lawrie/CS774/S06/homework/klm.pdf

15. Overill, R.E., Silomon, J.A.M., Chow, K-P, A Complexity Based Model for Quantifying Forensic Evidential Probabilities, Proc. 3rd International Workshop on Digital Forensics (WSDF 2010), Krakow, Poland, pp.671–676 (February 2010)

16. Overill, R.E., Silomon, J.A.M., Digital Meta-Forensics: Quantifying the Investigation, Proc. 4th International Conference on Cybercrime Forensics Education & Training (CFET 2010), Canterbury, UK (September 2010)