C25 Quantum Digital Forensics: The Applications of Digital Forensics in a Quantum World

Suzzanne I. Myers, Silicon Valley Bank, Tempe, AZ 85281*

Learning Overview: After attending this presentation, attendees will have a better understanding of how quantum computers are poised to impact the future of digital forensic work. Attendees will gain an understanding of how quantum computers function and insight into both the advantages and disadvantages of their application to the digital forensic landscape.

Impact on the Forensic Science Community: As with any new technology, digital forensic examiners need to understand how it works and what the impact is to the data they sift through daily to best anticipate both the case applications and the security needs of their industry. This presentation will impact the forensic science community by encouraging discussion on the applications of quantum computers and better preparing the digital forensic community for the anticipated challenges and opportunities of working in a quantum world.

Digital forensic analysts are on the cusp of needing to fight a battle against exponentially more powerful cyber threats. What was once only considered science fiction is now reality, and quantum computers in the wrong hands present a significant problem for those trying to protect individuals and organizations from attackers. The applications for a quantum computer—such as the expansion of cloud computing, a faster internet, unbreakable encryption, and new channels of communication—are also rapidly generating interest in the security industry.[1]

There are significant differences between quantum and classical computers, and some of the problems forensic examiners will face are extracting live data from a system when that data can be in multiple states at the same time, creating exact forensic copies when the state of a bit can change with each observation, capturing data in a transmission when the packet doesn't ever traverse a network, and breaking encryption in a post-quantum environment.[2-4,7,8,10,12-14]

With these challenges also come opportunities. Digital forensic analysts will be able to use quantum encryption to crack old cases that classical computers simply couldn't solve.[5,6] They'll be able to use quantum's pattern-matching technology to scan large databases for matches on faces, locations, and objects of interest.[9] Finally, quantum computers will very likely facilitate the transmission of classical information, making it imperative for examiners to know and understand the architecture they are dealing with.[11,15]

This presentation examines the above questions and discusses the types of forensic needs necessary in a quantum world. This presentation will review how data will be transmitted in a quantum environment, advantages and disadvantages versus classical forensics, the potential for live forensics, pattern recognition for law enforcement applications, and discuss the code-breaking implications for today's current forensic encryption challenges.

Reference(s):

1. Shor, P. Quantum Information Theory: Results and Open Problems. Geometry Functional Analysis. *Special Volume—GAFA2000*, (2000):816-838.
2. Cao,Y., Li, Y., Cao, Z., Yin, J., Chen, Y., Yin, H., Chen, T., Ma, X., Peng, C., and Pan, J. Direct counterfactual communication via quantum Zeno effect. *Proceedings of the National Academy of Sciences of the United States of America (PNAS), PNAS Early Edition*, 1-5. (2017).
3. Cheng, Q., Wang, C., and Tao, M. Quantum Communication for Wireless Wide-Area Networks. *IEEE Journal on Selected Areas in Communications*, 23(7) (2005): 1424-1432.
4. Garipelly, R., Kiran, P.M., and Kumar, A.S. A Review on Reversible Logic Gates and their Implementation. *International Journal of Emerging Technology and Advanced Engineering*, 3(3), (2013) 417-419.
5. Jodoin, E. *Straddling the Next Frontier Part 1: Quantum Computing Primer.* SANS Institute, (Tech.), (2014).
6. Jodoin, E. *Straddling the Next Frontier Part 2: How Quantum Computing Has Already Begun Impacting the Cyber Security Landscape*. SANS Institute, (Tech) (2014).
7. G.B. Lesovik, I.A. Sadovskyy, M.V. Suslov, A.V. Lebedev, and V.M. Vinokur, (2019). Arrow of time and its reversal on the IBM quantum computer. *Scientific Reports*, 9(4396), (2019).
8. Overill, R.E. Digital Quantum Forensics: Challenges and Responses. *Future Information Technology: 6th International Conference, Part II*, (2011) 110-114.
9. Boyda E., Basu S., Ganguly S., Michaelis A., Mukhopadhyay S., Nemani R.R. Deploying a quantum annealing processor to detect tree cover in aerial imagery of California. *PLoS ONE* 12(2) (2017).
10. Van Zandwijk, J., and Fukami, A. NAND Flash Memory Forensic Analysis and the Growing Challenge of Bit Errors. *IEEE Security & Privacy*, 15, (2017): 82-87.
11. Wehner, S., Elkouss, D., and Hanson, R. Quantum internet: A vision for the road ahead. *Science*, 362(6412), (2018) 1-9.
12. Weng, J., Zhang, F., Sun, K., and Stavrou, A. Firmware-assisted Memory Acquisition and Analysis tools for Digital Forensics. *2001 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*. (2001).
13. Wooters, W.K. and Zurek, W.H. The No-Cloning Theorem. *Physics Today*, 62(2), (2009) 76. doi:10.1063/1.3086114.
14. Yanofsky, N.S. and Mannucci, M.A. *Quantum Computing for Computer Scientists.* Cambridge: Cambridge University Press. (2008).
15. Yakaboylu, E., Camus, N., Fechner, L., Klaiber, M., Laux, M., Mi, Y., Hatsagortsyan, K.Z., Pfeifer, T., Keitel, C.H., and Moshammer, R. Experimental Evidence for Quantum Tunneling Time. *Physical Review Letters*, 14. (2017).

Quantum Digital Forensics, Digital Forensics, Quantum Computers

Copyright 2020 by the AAFS. Permission to reprint, publish, or otherwise reproduce such material in any form other than photocopying must be obtained by the AAFS.

*Presenting Author