Chapter 9
The Role of Quantum Computing in Software Forensics and Digital Evidence: Issues and Challenges

Sandeep Kumar Sharma
https://orcid.org/0000-0002-2048-671X
Department of Computer Science and IT, Khwaja Moinuddin Chishti Language University, India

Mazhar Khaliq
Department of Computer Science and IT, Khwaja Moinuddin Chishti Language University, India

ABSTRACT

Quantum computing has immense computational advantages. It escorts today's world of computing towards qubits universe of computing by the logical superposition technique. Various new technologies will come to reality with replacement of existing problem-solving methodology. The development of quantum computing imposes significant impact on cyber security and digital forensics technologies. Cybercrimes may be dramatically increased and malicious code will get ability to harm speedily. The quantum computing in software forensics methodology needs to develop in order to counter the challenges such as traceability of malicious code automation, sources of malicious code generation, intellectual property right theft issues, source code validation, plagiarism, breach of copyright issues, and an acquisition of digital evidence with quality and quantity with the wings of quantum forensics. This chapter aims to concentrate on the key issues of quantum computing approach in the field of software forensics with ontological aspects.

DOI: 10.4018/978-1-7998-6677-0.ch009

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION AND BACKGROUND STUDY

The advances in information technology have a large effect on our digital life and digital society. Quantum computing is an exciting technological development for a world of opportunities with safe environment and sustainable development and implementation. Amazon has launched its "quantum as a service" as Amazon Braket for scientists, researchers and developers to build, test and run quantum computing algorithms. Quantum computing would be accomplished in resolving extraordinarily complex problems within one decade with supercomputer competency. It would lead to revolutionize a variety of fields, including cryptography, cyber-security, digital forensics, medical computing, and many more. Quantum computing a single qubit can in general be an unequal linear superposition of the basis states zero and one:

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

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

$\Psi >= > \otimes > \otimes \otimes >\equiv >$ n |1 |1 |1 |11 1 … …

"Applying a linear (n–1) number of operations to the qureg yields a register state which is a superposition of an exponential ($2n$) number of terms. This exponential performance is one crucial characteristic of the potential power of quantum computation." (Overill, 2012)

Quantum computing and the architecture of computation challenges to think differently in the world of computation. For quantum systems have to develop entirely new software coding languages, algorithms, measurement standards and a whole host of yet-to-be invented tools currently two technologies show great promise first superconducting qubits and second trapped ions.

The theory of quantum mechanics produces the fundamental principles of quantum computing. These fundamental concepts are superposition, entanglement and the uncertainty principle in quantum mechanical measurements. The theory of information that led to the development of quantum information theory, in which quantum computing originates alongside quantum communication and quantum sensing among many others. Any two (or more) quantum states can be added together ("superposed") and the result will be another valid quantum state; and conversely, that every quantum state can be represented as a sum of two or more other distinct states.

Quantum mechanics permits multiple register elements to collectively store superposition over multiple binary values. "This phenomenon, known as entanglement, is a form of information that cannot be reproduced by conventional bits. While the register elements remain independently addressable, the information they store can no longer be expressed piecewise. The principles of superposition and entanglement lead to an important conceptual difference about how to interpret the value of a register". Werner Heisenberg formulated the uncertainty principle at Niels Bohr's institute in Copenhagen, while working on the mathematical foundations of quantum mechanics. In quantum mechanics, the uncertainty principle is any of a variety of mathematical inequalities. (Sen, D., 2014)

"Asserting a fundamental limit to the precision with which the values for certain pairs of physical quantities of a particle, such as position, x, and momentum, p, can be predicted from initial conditions. The Heisenberg Uncertainty Principle states that the product of uncertainties in related physical quantities (e.g. position and momentum, energy and time, etc.) has a finite lower bound" (Bohr & Waldemar, 1958)

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/the-role-of-quantum-computing-in-software-forensics-and-digital-evidence/272370

Related Content

An Adaptive Security Framework for the Internet of Things Applications Based on the Contextual Information

Harsuminder Kaur Gill, Anil Kumar Vermaand Rajinder Sandhu (2019). *Cryptographic Security Solutions for the Internet of Things (pp. 244-267).*
www.irma-international.org/chapter/an-adaptive-security-framework-for-the-internet-of-things-applications-based-on-the-contextual-information/222278

LFSR-Keyed MUX for Random Number Generation in Nano Communication Using QCA

Padmapriya Praveenkumar, Santhiya Devi R., Amirtharajan Rengarajanand John Bosco Balaguru Rayappan (2020). *Quantum Cryptography and the Future of Cyber Security (pp. 70-83).*
www.irma-international.org/chapter/lfsr-keyed-mux-for-random-number-generation-in-nano-communication-using-qca/248152

The Role of Quantum Computing in Software Forensics and Digital Evidence: Issues and Challenges

Sandeep Kumar Sharmaand Mazhar Khaliq (2021). *Limitations and Future Applications of Quantum Cryptography (pp. 169-185).*
www.irma-international.org/chapter/the-role-of-quantum-computing-in-software-forensics-and-digital-evidence/272370

Efficient Implementation of Digital Signature Algorithms

Sumathi Doraikannan (2018). *Algorithmic Strategies for Solving Complex Problems in Cryptography (pp. 78-86).*
www.irma-international.org/chapter/efficient-implementation-of-digital-signature-algorithms/188514

Quantum Cryptography for Securing IoT-Based Healthcare Systems

Anand Sharmaand Alekha Parimal Bhatt (2021). *Limitations and Future Applications of Quantum Cryptography (pp. 124-147).*
www.irma-international.org/chapter/quantum-cryptography-for-securing-iot-based-healthcare-systems/272368