Thesis Proposal

Sammy Al Hashemi (1001548337)

The idea of a quantum computers was first proposed by Richard Feynman in 1982, as a possible solution to solve programs that could not be solved in polynomial time on a classical computer [1]. This sentiment has inspired a movement in favour of development of large-scaled quantum computers and has recently risen to the forefront in many tech giants such as Google, IBM, Microsoft, and Alibaba [2]. Recent preliminary results on smaller-scale quantum processors with up to 20 qubits have demonstrated the capability of the hardware to be programmed and controlled. The biggest challenge lies ahead in efforts to reduce the hardware limitations currently available. This is an incredible challenge going forward as it requires physical qubits well isolated from the environment and capable of being addressed and coupled to more than one extra qubit [3]. However, there has been massive progress recently, as the largest tech giants compete to build the first commercially available quantum computer [2]. For example, Google recently announced Bristlecone, their new 72-qubit quantum processor while Rigetti announced their own 128-qubit chip [14]. Although Google is ‘cautiously optimistic’, this is very exciting as it has been proposed that quantum devices with more than ~50 qubits are expected to perform certain algorithms better than classical computers, thus achieving quantum supremacy [4][5].

The implications of the emergence of quantum computing are very great, particularly when considering the strength of modern data security for major companies, banks and blockchains [7]. Two quantum algorithms that are of utmost importance in this context are Shor’s (prime factorization) and Grover’s (unstructured database query) algorithms [9][13]. Classical computers do not possess the power to overcome the computational effort required to break modern encryption methods, which in the case of RSA key encryption, require the prime factorization of very large numbers, and lattice-based encryption schemes often require solving a variant of the shortest vector problem (SVP). The emergence of Shor’s algorithm is currently of main concern due to its threat on the most popular encryption algorithms, such as RSA encryption. Grover’s algorithm presents further threats to encryption algorithms proposed in response to Shor’s, due to its ability to solve cryptographic hashing and ease the complexity in solving SVP and AES encryption [6][7][8].

While Grover’s algorithm is a clearly defined problem, and early versions do exist, there is room to invest in its practicality and scalability, as quantum computers continue to evolve past their current limitations. Grover’s algorithm assumes the existence of a “magical” black-box oracle function that identifies when any “winning” value exists, while searching in an unstructured database [9]. Early implementations use quantum circuits with oracles precompiled for predefined values [9][10][11][12]. The objective of this research, is to develop a practical oracle function for use in Grover’s algorithm in any scalable system and create benchmark tests to estimate and measure the runtime on actual hardware. To do so, and initial step of extensive literature review, and public consultation of forums specific to the quantum computing community, is considered. To test and validate what has been done, small-scale circuits will be built for execution on currently available simulation engines such as Rigetti Forest and IBM Quantum Experience. The hardware will be accessed through IBM Quantum Experience’s 16 qubit processor available for public use over the cloud using their python SDK. For each test attempted, the complexity and accuracy of each presented oracle will be judged. Once confident that a valid practical implementation of an oracle has been demonstrated, the remainder of the paper will deal with introducing parameterization for scalability of the algorithm.

Citations:

[1] Deutsch, D. and Ekert, A. (1998). Quantum computation. *Physics World*, 11(3), pp.47-52 [Accessed 12 10 2018].

[2] D. Castelvecchi, "Quantum computers ready to leap out of the lab in 2017," 03 January 2017. [Online]. Available: http://www.nature.com/news/quantum-computers-ready-to- leap-out-of-the-lab-in-2017-1.21239. [Accessed 12 10 2018].

[3] J. M. Gambetta, J. M. Chow, and M. Steffen, "Building logical qubits in a superconducting quantum computing system," *npj Quantum Information*, vol. 3, no. 1, 2017 [Accessed 12 10 2018]

[4] S. Boixo, S. V. Isakov, Vadim N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis and H. Neven, "Characterizing Quantum Supremacy in Near-Term Devices," *arXiv:1608.00263v3 [quant-ph]*, [Accessed *12* 01 2018].

[5] J. Kelly, "A Preview of Bristlecone, Google's New Quantum Processor", *Google AI Blog*, 2018. [Online]. Available: https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html. [Accessed: 13- Oct- 2018].

[6] S. Ray, "Quantum Threat to Blockchains: Shor's and Grover's Algorithms," *codeburst*, 22-Jul-2018. [Online]. Available: https://codeburst.io/quantum-threat-to-blockchains-shors-and-grover-s-algorithms-9b01941bed01. [Accessed: 13-Oct-2018].

[7] Wickr, "What is Lattice-based cryptography & why should you care," *Wickr*, 15-Jun-2018. [Online]. Available: https://medium.com/cryptoblog/what-is-lattice-based-cryptography-why-should-you-care-dbf9957ab717. [Accessed: 13-Oct-2018].

[8] T. Laarhoven, M. Mosca, and J. V. D. Pol, "Solving the Shortest Vector Problem in Lattices Faster Using Quantum Search," *Post-Quantum Cryptography Lecture Notes in Computer Science*, vol. 1, no. 6176, pp. 83–101, Jan. 2013.

[9] L. Grover, "A fast quantum mechanical algorithm for database search," *arXiv:quant- ph/9605043*, 1996.

[10] K.A Brickman "Implementation of Grover's Quantum Search Algorithm with Two Trapped Cadmium Ions" pHD Thesis, University of Michigan, Ann-Arbour, Michigan, 2007 [Accessed: 13 Oct 2018].

[11] K.-A. Brickman, P. C. Haljan, P. J. Lee, M. Acton, L. Deslauriers, and C. Monroe, "Implementation of Grover's quantum search algorithm in a scalable system," *Physical Review A*, vol. 72, no. 5, 2005.

[12] C. Figgatt, D. Maslov, K. A. Landsman, N. M. Linke, S. Debnath, and C. Monroe, "Complete 3-Qubit Grover search on a programmable quantum computer," *Nature Communications*, vol. 8, no. 1, Mar. 2017.

[13] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *arXiv:quant-ph/9508027,* 1996.

[14] R. Computing, “The Rigetti 128-qubit chip and what it means for quantum,” *Medium*, 08-Aug-2018. [Online]. Available: https://medium.com/rigetti/the-rigetti-128-qubit-chip-and-what-it-means-for-quantum-df757d1b71ea. [Accessed: 15-Oct-2018].