Demonstration and Implementation of Quantum Computing in Cryptanalysis

Yiran Zhao*

Department of Physics, Fudan University, Shanghai, China

*Corresponding author: 20307110062@fudan.edu.cn

Abstract. Quantum computing has long been a hot topic in both fields of physics and computer science. As a matter of fact, most of the earliest quantum algorithms are related to cryptology on account of its potential advantage over conventional computers. In this paper, Bernstein-Vazirani algorithm, a linear cryptanalysis method performing on quantum computers, is selected as a typical algorithm to demonstration and implementation of the quantum computing in cryptanalysis. To be specific, this study analyzes the method itself, and realizes the method with Qiskit so as to compare it with conventional methods. With the comparison, the superiority of quantum computing in certain fields as well as some current disadvantages to be dealt with are clarified. Thus, it is hoped to present the huge potential of quantum computing in its processing ability and its property of superposition beginning with the field of cryptanalysis. Besides, a direction of future improvement of the technology is also proposed. Overall, these results shed light on guiding further exploration of quantum computing.

Keywords: Quantum Computing; Cryptanalysis; Qiskit; Bernstein-Vazirani algorithm.

1. Introduction

Conventional computer development has been obstructed due to the limits on its fundamental factors, including manufacturing, energy, chip size and designing, algorithms etc. [1, 2]. For example, owing to the quantum tunneling effect, the size of a silicon chip is not limited by the accuracy in manufacturing, but the laws of quantum mechanics [3, 4]. Conventional computers also suffer from low efficiency when dealing with high dimensional data even with efforts in improving the algorithms because of its binary system [5]. Although the invention of machine learning, deep learning and artificial intelligence seems to boast the industry in various fields, it takes much more efforts to satisfy Moore scaling nowadays [6-8]. The development of conventional computers has met a choke point. Therefore, a shift from conventional computing to quantum computing is necessary in order to offer the improvement in computing efficiency with the needs of processing data and solving problems.

Richard Feynman described a quantum machine based on the laws of quantum mechanics in 1982, which is widely regarded as one of the earliest ideas for quantum computing [9]. Because nature is not classical, natural phenomena simulation requires a computer working on quantum mechanical principles. A quantum computer can take advantage of special properties of quantum mechanics (e.g., entanglement and superposition), which is capable of calculating complex quantum systems.

The most fundamental difference between a quantum computer and a conventional one is the quantum bit, or qubit. Unlike a binary bit, which can only be either 0 or 1 at one time, a qubit can be a linear combination of the two states. This phenomenon is called superposition in physics. The spin of an electron, the polarization of a photon and the ground state and excited states of a quantum system are some examples of it. Therefore, a qubit represents a linear combination of complex numbers with amplitude and phase. As shown in Fig 1, the 'value' of a qubit can be better understood through spherical coordinates, which is also the basis of quantum programming. At first, the development of quantum computers was rather slow, because scholars didn't understand much about quantum mechanics and how to manipulate quantum states [10-12]. The decoherence of qubits is another challenge. Any slight changes in the environment, like temperature and magnetic field, will cause the qubits decohere to classical bits. However, the past decade has witnessed rapid progress in the field of quantum computing. The great potential of quantum computing capabilities surpassing

supercomputers inspires both industry and academia to realize it by building a functional and programmable quantum computer. Companies including IBM, Microsoft and Google have been devoted to the development of their quantum computer in recent years.

Meanwhile, the development of quantum algorithm has also experienced considerable progress based on the development of the hardware. Comparing to the early 90's, when there were only very few algorithms that are suitable for quantum computers, such as the famous Shor's algorithm, today there are hundreds of quantum algorithms ready to fulfil the potential of quantum computing. This study focuses on the Bernstein-Vazirani algorithm, a basic decoding algorithm based on quantum computing, and compare it with a conventional decoding algorithm [13, 14]. By showing the complexity of the calculation, one can have a glimpse of the potential of quantum computing and the changes it will bring about, as well as the defects that we still need to work on.

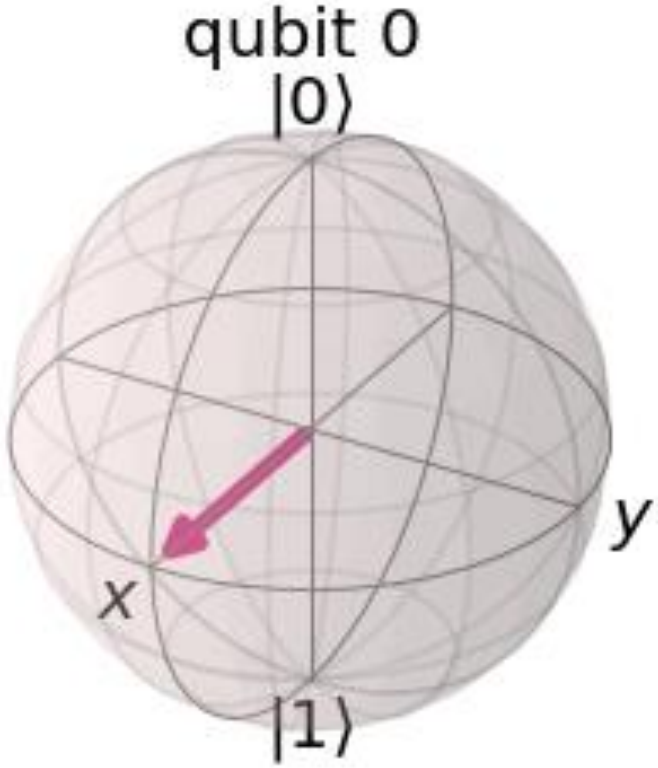

Fig 1. A qubit representing the linear combination of states $|0\rangle$ and $|1\rangle$. In this case, the probability of both states is 50%.

2. Algorithms and Platforms

2.1. Algorithm Description

The Bernstein-Vazirani algorithm this study focuses on is rather basic, but can effectively show the great difference between quantum computing and conventional computing [15]. This study will first introduce this algorithm. Consider a Boolean function f whose input is an n-digit binary number x, and the output is 0 or 1:

$$f(x_1x_2,\cdots x_n) \to 0 \; or \; 1. \tag{1}$$

The output is determined by an n-bit sequence $s \in \{0,1\}^n$ with the function:

$$f_s(x) = s \cdot x \; (\text{mod } 2). \tag{2}$$

The Bernstein-Vazirani problem, accordingly, is to calculate the n-bit sequence s, known as the 'code' of this function. One now tries to find s with both conventional and quantum computing methods.

With the conventional computing method, the most convenient way is shown below. One needs to input the unit matrix sequences in turn in order to find the value of each digit of s. The ith input helps us find the ith digit of s:

$$f_s(x) = s \cdot x \,(\mathrm{mod}\ 2) = s_i. \tag{3}$$

Therefore, it takes at least n steps for conventional computing methods to find the code s.

With quantum computing, there is a completely novel approach to the problem. The first step is to initialize the state of $(n+1)$ qubits:

$$|\psi_1\rangle = |0\rangle^{\otimes n}|1\rangle, \tag{4}$$

And then one performs the Hadamard transform H^{n+1} on the $(n+1)$ qubits:

$$|\psi_2\rangle = H^{\otimes(n+1)}|0\rangle^{\otimes n}|1\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{5}$$

Subsequently, one performs the function f on the state. The physical process is actually one hardware functioning on the qubits:

$$|x\rangle|a\rangle \to |x\rangle|a \oplus f(x)\rangle. \tag{6}$$

Therefore, the state becomes:

$$|\psi_3\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle). \tag{7}$$

The operator $\oplus$ here stands for 'exclusive or'. We can further calculate Eq. (7) as

$$|\psi_3\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle). \tag{8}$$

Now, one ignores the last qubit, and perform the Hadamard transform H^n on the rest qubits:

$$|\psi_4\rangle = H^{\otimes n} \cdot \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}|x\rangle = H^{\otimes n} \cdot \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{s\cdot x}|x\rangle = H^{\otimes n} \cdot H^{\otimes n} \cdot |s\rangle = |s\rangle \tag{9}$$

Finally, all one needs to do is to measure the quantum state, and we will get the code s. The description seems quite complicated, but the calculation is extremely simple for a quantum computer.

2.2. Platforms

In this paper, all quantum algorithms are based on Qiskit, an open-source software development kit (SDK) for working with quantum computers developed by IBM. Due to the constraint of IBM Quantum, the result would be the simulation of the code instead of the real result from actual quantum computers. The backends for simulation we used are 'qasm_simulator' and 'statevector_simulator'. There will be some slight differences, since the simulation is based on the ideal condition with no noise. In fact, for most algorithms, the noise may have some great impact on the result, but in this case the noise has very little contribution to the result.

3. Results & Discussion

3.1. Results

With Qiskit, one can easily realize the algorithm concerning the Bernstein-Vazirani Problem. When coding the quantum program, it is assumed that the code s is a 6-digit binary number and users need one additional qubit according to the method mentioned above. Thus, 7 qubits are required altogether in order to solve the 6-digit-code problem. Using matplotlib and qiskit.tools.visualization, one can visualize the algorithm discussed above. With a given code s, for example '101001', the quantum circuit is visualized as illustrated in Fig 2.

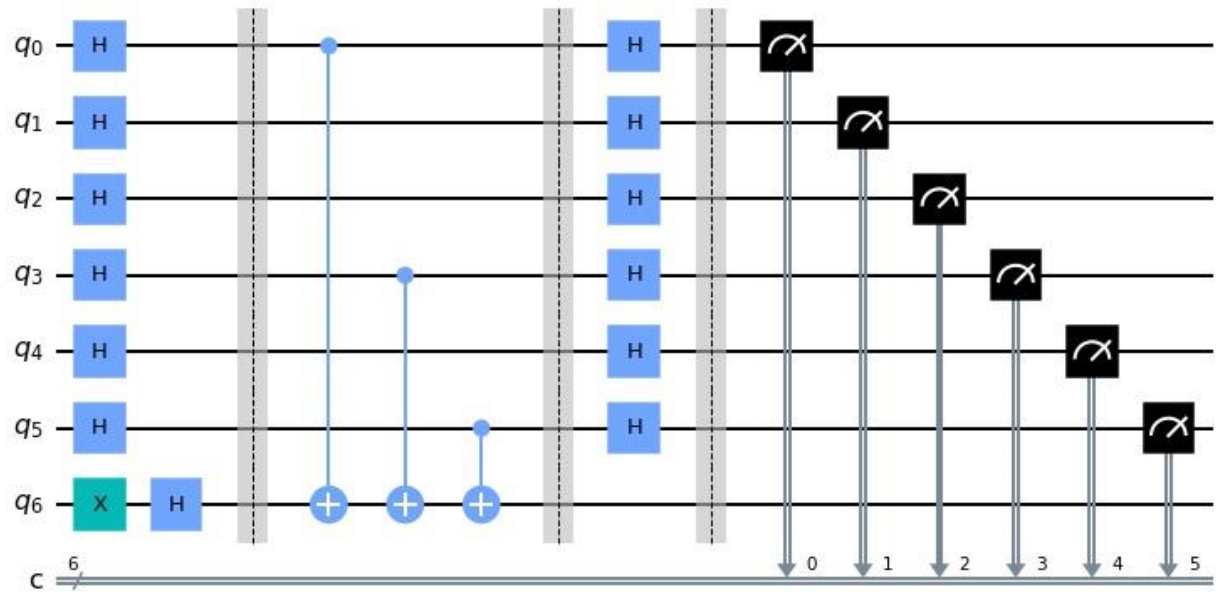

Fig 2. The quantum circuit of Bernstein-Vazirani algorithm, presented with Qiskit. In this case, the code is 101001, measured by qubits $q_5, q_4 \cdots, q_0$.

In the circuit, $q_0, q_1, \cdots, q_5$ are qubits used for storing the code (in other words, presenting the Boolean function), and q_6 is used to interact with the former 6 qubits according to the function, as Eq. (4) shows. The left side of the first barrier represents the initialization of qubits. After the first barrier is the process where the code acts on the qubits, and thus the function has been constructed on the quantum computer. Afterwards, the Hadamard gates are applied to the 6 qubits. According to Eq(9), all one has to do is to measure the state of the qubits, and one will get the code.

3.2. Comparison

The quantum computing method of Bernstein-Vazirani algorithm in solving the problem is very convenient to apply. The algorithm complexity of the method is $O(1)$. This is incredible, because it is irrelevant to the length of the code. No matter how long the code is, one step of calculation on a quantum computer can find the solution. On the contrary, as we have shown in section 2.1, the algorithm complexity of the conventional computing method is $O(n)$. When handling a long code, there will be distinct disparity in the speed of quantum computing and conventional methods. This implies that quantum computing has huge potential in solving certain problems that current conventional computers may have difficulty processing, or the efficiency of conventional methods is far from satisfactory.

3.3. Application

The Bernstein-Vazirani algorithm itself seems limited in application. However, the quantum method it used in attacking block ciphers is quite improvising [16]. In the field of cryptanalysis,

similar methods based on Bernstein-Vazirani algorithm have already been making contributions. Many conventional cryptology methods have been easily conquered by these quantum algorithms, including the Feistel scheme, Even-Mansour construction and so on. In fact, most of the earliest quantum algorithms (e.g., Shor's algorithm) were devoted to cryptology, and has already promoted the research in the field [17].

4. Limitation & Prospects

From the former discussion, one can easily understand the merits of quantum computing comparing with conventional methods. At the same time, some disadvantages of quantum computing have also been exposed. For one thing, the simple Bernstein-Vazirani algorithm requires (n+1) available qubits to deal with an n-digit code problem. The longer the code is, the larger the quantity of qubits one needs. This will be a big challenge when n is close to or even greater than a hundred. One problem is the technology in manufacturing. Currently, IBM boasts the 127-qubits quantum computer, which is the largest one globally. Any improvement would be extremely difficult, since the preservation of qubits requires an accurate control of environment. Another problem is concerned with the decoherence of qubits. With a larger quantity of qubits, any slight disturbance will lead to decoherence of the superposition of qubits. The accumulation of noise will also bring about mistakes in the result. These are all factors constraining the application of quantum computing. As discussed in section 3.2, the advantage of quantum Bernstein-Vazirani algorithm over conventional ones is only significant when the length of the code is long enough. But for now, our quantum computers are unable to deal with the problem in such an efficient way. For another, one should not focus only on the complexity but also the energy consumption of quantum computing. Although it costs less time for a quantum computer to cope with certain problems, the energy and expenditure using to maintain and run a quantum computer, as mentioned above, is far more than what it costs to run a conventional computer.

However, the future of quantum computer is still very promising despite these demerits. The hardware manufacturing of quantum computers is an investment hot spot, and many institutions and businesses are devoted to the construction. Hopefully, one will have a 1000-qubit computer in a few years according to IBM Summit 2022. Tthanks to the special property of superposition, the ability of storing and processing data of qubits would increase exponentially as the quantity of qubits increases. According to the estimation the processing ability of a quantum computer with 60 qubits will surpass existing super computers. Therefore, current flaws of quantum computing can be fixed in several years, and one still cannot see its full potential. The era of quantum computing is bound to come, and human beings will witness the huge changes it will bring about.

5. Conclusion

In summary, this study have discussed the Bernstein-Vazirani algorithm based on quantum computing used for linear cryptanalysis. To be specific, the principles of the algorithm and realization the coding with Qiskit are demonstrated. By comparing the quantum method with conventional ones, the superiority of quantum computing in certain fields is clarfied. In addition, some current disadvantages of quantum computing are presented, which will constrain the use of quantum computers in various conditions. Unfortunately, it is unable to run the program on IBM Quantum Computer, and thus the effect of noise has not been well researched. It is hoped that this paper will help reseachers aware of the basic quantum cryptanalysis theory, and learn its merits and demerits so as to further develop the theory as well as the hardware of quantum computing. Overall, these results offer a guideline for quantum computing algorithms applications.

References

[1] Markov Igor L. Limits on fundamental limits to computation. Nature 2014, 512.7513: 147-154.

[2] Morton J. L, et al. Embracing the quantum limit in silicon computing." Nature, 2011, 479.7373: 345-353.

[3] Plummer J. D., and Peter B. G. Material and process limits in silicon VLSI technology. Proceedings of the IEEE, 2001, 89.3: 240-258.

[4] Liu Jun, et al. Sustained electron tunneling at unbiased metal-insulator-semiconductor triboelectric contacts. Nano energy, 2018, 48: 320-326.

[5] Yi Xinyang, Constantine Caramanis, and Eric Price. Binary embedding: Fundamental limits and fast algorithm. International Conference on Machine Learning. PMLR, 2015.

[6] Guo Yanming, et al. Deep learning for visual understanding: A review. Neurocomputing, 2016, 187: 27-48.

[7] Jordan M. I., and Tom M. M. Machine learning: Trends, perspectives, and prospects. Science, 2015, 349.6245: 255-260.

[8] Brunette E. S., Rory C. F., and Claire L. F. A review of artificial intelligence. 2009 4th International Conference on Autonomous Robots and Agents. IEEE, 2009.

[9] Feynman R P. Simulating Physics with Computers. International Journal of Theoretical Physics, 1982, 21.

[10] Gill Sukhpal Singh, et al. Quantum computing: A taxonomy, systematic review and future directions. Software: Practice and Experience, 2022, 52.1: 66-114.

[11] Gyongyosi Laszlo, and Sandor Imre. A survey on quantum computing technology. Computer Science Review, 2019, 31: 51-71.

[12] Yanofsky N. S. An introduction to quantum computing. Proof, computation and agency. Springer, Dordrecht, 2011. 145-180.

[13] Andersson M. P., et al. Quantum computing for chemical and biomolecular product design - ScienceDirect. Current Opinion in Chemical Engineering, 1996.

[14] Bernstein Ethan, and Umesh Vazirani. Quantum complexity theory. Proceedings of the twenty-fifth annual ACM symposium on Theory of computing. 1993.

[15] Nagata Koji, et al. A generalization of the Bernstein-Vazirani algorithm. MOJ Ecol. Environ. Sci., 2017, 2.1: 00010.

[16] Xie Huiqin, and Li Yang. Using Bernstein–Vazirani algorithm to attack block ciphers. Designs, Codes and Cryptography 2019, 87.5: 1161-1182.

[17] Rosenberg Nathanial O. Cryptology Management in a Quantum Computing Era. NAVAL POSTGRADUATE SCHOOL MONTEREY CA, 2012.