2021 IEEE 5th International Conference on Cryptography, Security and Privacy

Quantum Algorithms: Overviews, Foundations, and Speedups

Shuangbao Paul Wang
Department of Computer Science
Morgan State University
Baltimore, USA
paul.wang@computer.org

Eric Sakk
Department of Computer Science,
Morgan State University
Baltimore, USA
eric.sakk@morgan.edu

***Abstract*—This paper discusses quantum computing with a strong focus on quantum software, quantum networks, quantum simulation, and applications. The study on quantum speedups reveals fundamental differences between quantum algorithms and classical algorithms. As a case study, further improvement on Shor's algorithm is presented with experimental results. The study shows that quantum circuits can be generated automatically to further improve the efficiency of quantum algorithms.**

***Index Terms*—quantum algorithm, quantum computing, quantum cryptology, quantum cryptography**

I. Introduction

Quantum algorithms can make full use of powerful quantum computers that are to be built in the next decade or so. Today's computer systems and networks have vulnerabilities that provide a playground for hackers. Cache and pipelines improve the performance of computer systems but are vulnerable to side channel attacks that could lead to leaking data among the supposedly "isolated" virtual machines. Strong public encryptions provide convenience for key exchanges and "unbreakable" complexity to digital computers. However prime numbers are under attack by quantum computers where quantum algorithms can run considerably faster to make the impossible possible. Quantum Internet uses quantum communication satellites to entangle particles that exhibit "spooky action at a distance". Quantum key distribution (QKD) provides a more secure way of key exchanges that is immune to man-in-the-middle and other exploits. Quantum communication enables quantum networks to transfer entangled quantum states directly between nodes without actually transmitting a single physical qubit, thus further improving the security.

In the following sections, we first introduce quantum computing with a strong focus on quantum software, quantum networks, quantum simulation, and applications in cryptography, cryptology, and cybersecurity. We then look into the quantum speedup for some software and algorithms. Recent studies on efficient quantum algorithms are discussed and then combined with recent experimental results.

This research is funded by a grant from the National Science Foundation NSF #1560214.

II. Quantum Computing

Many people know that the atomic clock at the National Institute of Standards and Technology (NIST), few people realize that it was based on quantum technology until recently. Quantum entanglement and superposition were not main topics as they were merely discussed in books and technical papers. Now technologies based on quantum mechanics are used in building quantum computers, quantum networks, quantum random number generators (QRNG), and security devices such as quantum key distribution.

The superconducting quantum interference device was first developed at Ford research lab. This exquisitely sensitive magnetic-field sensor was later widely used in the MRI machines and other industrial devices. The current effort on quantum computing is not only fully funded the government and national labs, it is also backed by private sector and academia that provides training and education to college or even high school students. The trend of quantum workforce development is imminent and has been put at the national interest by many developing countries. Companies such as British company E2v manufactures quantum devices that can perform far beyond the current state of art. Technologies can discharge photons one at a time, considering 10^{20} photons emit from a 60 watt light bulb every second. It was unthinkable years ago. "Quantum supremacy" is no longer far to reach, as Google and some other companies have claimed to have reached the limit, though with disagreements from other companies. Therefore, engineers need to learn quantum to be competent in the quantum workforce. So far, quantum technology has penetrated into many industrial areas such as aerospace, manufacturing, banking, medicine, communication, cybersecurity, and many more. Without catching up with this new technology, industry or even nations would worry to fall behind.

Some computer scientists and cybersecurity professionals consider that we may have reached the "peak" of digital revolution but still cannot safe guard our information systems and data. Hackers are able to do things that we would have never thought about. The constant fight with such adversaries is cause to consider improvements for securing data. With inventions in architecture security and books in Computer

978-1-7281-8620-7/21/$31.00 ©2021 IEEE

Architecture and Security, researchers started to seek new territory. Quantum was the top choice to step into the new frontier of the computing field. Computer scientists are in a position to enhance and improve the efficiency of quantum algorithms, quantum cryptology, and quantum cryptography. The effort is seen as starting pay off with research and publications in the quantum algorithm field.

A. Quantum Software

The IBM vice president Dario Gil one said "The power of quantum computing is rediscovering all the problems that computers cannot solve, and having a path to solving them.". There are many facts that seem to support the claim.

For people study body CT scanner, it may not hard to understand the mechanics and mathematical foundation. But when people tune into MRI, they discovered that it is a new territory that involves spinning hydrogen proton along an axis. The magnetic field can change the rotating direction and protons are in "up" and "down" positions following the quantum mechanics. Radio frequency signals can disturb or flip the protons and when the frequency equals, they exchange energy by resonance with each other (to absorb energy). When the RF signals turned off, the protons flip back and energy is released. This is similar with phase in quantum computing. It is more fascinating that the 1977 invention (MRI) can be improved with a quarter of the cost but be 40 times faster with the help of nanoscale diamonds with nitrogen vacancies technology developed by a German company NVision.

On another medical ground, positron emission tomography (PET) record images of high energy gamma-ray light flying out of injected radioactive tracers. Quantum entanglement tomography is able to entangle the two opposite direction photos ejected from tissues. The entangled pair would be easily be identified by the location it came from. The can takes less time and radioactive material.

Shor's algorithm depicts an important case that quantum computing can solve problems that traditional computers cannot solve [1], [2]. The algorithm is able to reduce the computational complexity from unsolvable exponential to polynomial $O(n^3)$. Wang have acquired an NSF grant to speed up Shor's algorithm from computational thinking perspective aiming to factor multiple prime numbers in one program [3]. As we know each Quantum Fourier Transform (QFT) requires a (different) quantum circuit to run. Automatic quantum circuits generation (from various QFT) would make the "attack" on RSA possible when powerful quantum computers are ready.

B. Quantum Network

"The future of the technology lies in quantum networks." The Economist article "Quantum Technology is Beginning to Come into its Own" depicts quantum networks will connect major metropolitan areas with improved security, thanks to the "no observation" principle for the entangled qubits, and maybe faster in speed.

At Switzerland, the ID Quantique company has setup quantum links between data centers of financial institutions 50 km away. In UK, a 250 km quantum network has been deployed between the cities of Bristol, London, and Cambridge. The Quantum key distribution enabled network enables encryption of 100 Gbps data traffic with rapidly refreshed quantum keys. China has an even more ambitious agenda. It links Beijing, Jinan, and Shanghai with more than 50 nodes and covering 70 square kilometers. China's QKD enabled satellite quantum network transport quantum states to Urumqi with some 3,000 km away from Beijing and Shanghai.

The Switzerland quantum network mentioned about is a good example of using quantum network to address security concerns of real world applications – banking. Cambridge quantum network aims to improve data security with seamless user interaction using existing fiber network. Though it can only support thousands of uses with low (1 kbps) key rates per use, it shows a clear path for implementing quantum level security over metropolitan networks. China seems leading the game with its satellite quantum network. It can overcome the 200 km distance limitation of fiber-optical signals, while perfect quantum repeaters are issues due to the "no copy" and "temporarily decryption" at repeaters issues.

The expansion of quantum networks especially satellite quantum networks could lead to the next generation Internet – Quantum Internet with improved security to prevent man-in-the-middle attacks and other types of network intrusions.

Yet entangled qubits may vulnerable to environmental factors and signal decay. The qubit fidelity may degrade. Repeaters may expose keys during the "temporarily decryption" process. At the results, all security seems to rely on the QKD which may be a concern of "single point failure", as some researchers argues the strength of QKD over the best classical alternatives. In summary, the advancement in quantum technologies and quantum networks will eventually improve network communication security significantly. It is one of the first areas that quantum technologies can be used to solve todays security problems. More study on QKD is recommended in order to be sure it delivers the security we have expected.

1) Quantum Teleportation: Quantum teleportation is to transfer the quantum state of a particle from one to another and erase the original state after transmission/teleportation. Quantum teleportation is able to not only transmit the quantum state of a photon from one place to another photon in another place that is hundreds kilometers away, it also can transmit the quantum state between earth and a satellite some 1,400 km apart. Quantum entanglement is the key to make the teleportation happen.

The quantum teleportation begins by using an entangled pair of photons. One photon (A) is held by Alice, the sender, and another one (B) to send to Bob, the receiver. Alice also has another photon (C) that she doesn't know the state to teleport to Bob.

After a Bell measurement on A and C at Alice side, photon B can be transformed in a state that has the initial state of C at Bob site. Note on the Alice side, since she measures C, it destroys the state for C.

The question is what kind of operations are needed for Bob to get photon B's state to be the same as that of C? In the teleportation protocol, Alice sends the C's state information via classical channel. When Bob receives the instructions, he know how to transform B into a state that is identical to the initial state of C. Figure 1 illustrates the teleportation process between Alice and Bob.

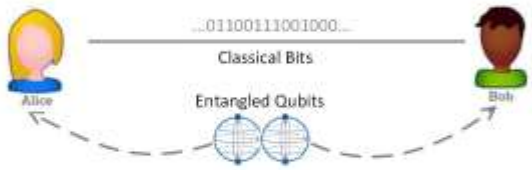

Fig. 1. Quantum Teleportation

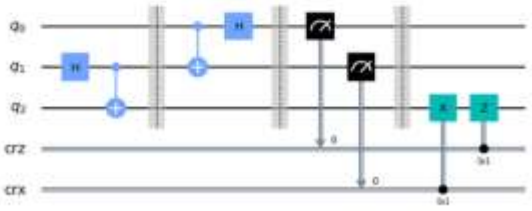

Fig. 2. Quantum Circuit for Teleportation

Figure 2 shows the quantum circuit of the quantum teleportation generated using IBM *qiskit*.

As we can see there is no time factor during the teleportation. It is therefore reasonable to think that teleportation can be faster than the speed of light, which Einstein described as "spooky action at a distance". In reality the teleportation speed cannot exceed the speed of light as the process need to transmit information through the classical channel.

2) Quantum Key Distribution: Since quantum states cannot be observed without destroy the quantum state, the property can be used to improve the security of network communication. In cryptography, cryptographic key exchange process may expose the key to intruders. Quantum key distribution can prevent such attack such has man in the middle attack. Any attempt to "observe" the quantum states will lead to errors at the recipient's side, which indicates there were eavesdroppers.

Networks using QKD still need a classical fiber channel or satellite channel for transmitting and receiving data. QKD is used to distribute keys and in case a higher error rate arise. Figure 3 shows a QKD diagram.

C. Quantum Simulation and Applications in Cybersecurity

Quantum computing utilizes quantum physics theory to manipulate entangled states. Operation on one qubit will result in all states change that may lead to converge to a possible solution after measurements. The qubits represents information in far greater numbers than binary. If errors can be controlled

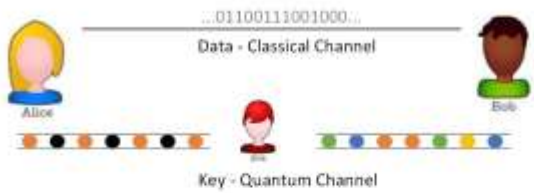

Fig. 3. Quantum Key Distribution - A Quantum Channel for Key distribution and a Classical Channel for Data Communication

to minimum, it can solve many unsolvable programs (eg. exponential in computation) with linear or polynomial speed.

Quantum simulation is one of the areas that draws attentions by academia, corporations, and government [4]. Room-temperature superconductors may be possible by means of quantum simulators. One of the advantages is that it will make the 600+ km/h Maglev train more available running in cities and interstates. All farm plants need fertilizer to grow. As a key ingredient, nitrogen simulation can investigate deep into the reactions to grow more crops. Battery is another important type energy that powers the cell phones, electric vehicles, and many other electronic devices. Bosch uses quantum simulations in helping design better batteries that can have more energy, last longer, and fast charge speed. Airbus uses quantum simulations to develop lighter material that makes the design and development process much fast and cheaper. The performance cold be a couple of orders of magnitude. Currently more small quantum computers are come to earth, some special purpose quantum computers, such as those at D-Wave have extraordinary speed advantage and they are totally different and better than classical computers. IBM Quantum Experience allows anyone to program on small quantum computers using visual programming interface (*Composer*). In addition, it also allow more experienced uses to program using Qiskit in the cloud (*Quantum Lab*), an interesting pilot in quantum cloud computing. Using trapped ion to build quantum computers is promising. IonQ is able to make it commercial use of trapped ion quantum computers. By manipulating individual atoms, it has the potential to "solve" real-world problems in medicine, chemistry and more.

From computer science perspective, improving computer and network security is one of the top tasks we are facing today. With the potential to break RSA using the Shor's algorithm on future large scale quantum computers, we have to compete with our adversaries in quantum computing to take the advantage in information security. There are nation states that "record" all data on fiber-optic networks hoping one day they can reveal today's top secret, which would still threat the national security. Research and development of quantum computing and efficient quantum algorithm will guarantee to win the war and guide the cyberspace. Investing quantum computing now will also include to educate high school and college students to enter the quantum job market when the "quantum supremacy" is ready.

III. Quantum Algorithms and Speedups

There are many things in common between classical algorithms and quantum algorithms [5], [6]. They both perform initialization, take input data, perform computing, and yield results for users to read or measure. On the other hand, there are many differences that programmers should keep in mind. Classical computers mostly follow the von Neumann architecture [7], which use binary and logic operations. Quantum computers, however, use qubits with superposition, entanglement, and interference to form quantum operations. Results from classical computers are deterministic while results from quantum computers are probabilistic. In order to reduce errors, quantum computers need to run considerable large number of times to get a statistical result.

A. The Deutsch-Jozsa Algorithm

The Deutsch-Jozsa algorithm demonstrate quantum speedup for a Boolean function. The oracle would tell you whether the output of the Boolean function is constant (either all 0 or all 1) or balanced (half 0 and half 1).

For n inputs, classical algorithm needs to compute $2^{n-1}+1$ time to determine whether it is a constant oracle or balanced oracle. Using quantum algorithm, however, only one step is required. So the speedup is exponential.

B. Quantum Fourier Transform

Shor's algorithm reduces the computation complexity factor large prime numbers from exponential to polynomial. The core speedup is at the Quantum Fourier Transform step.

The QFT follows the footsteps of Discrete Fourier Transform (DFT) and Fast Fourier Transform (FFT).

The DFT maps a vector of complex numbers $(x_0, x_1, ..., x_{N-1})$ to another vector of complex numbers $(y_0, y_1, ..., y_{N-1})$ defined by

$$\begin{aligned} y_k &= \sum_{j=0}^{N-1} x_j \cdot e^{-\frac{i2\pi}{N}kj} \\ &= \sum_{j=0}^{N-1} x_j \cdot \left[\cos\left(\frac{2\pi}{N}kj\right) - i \cdot \sin\left(\frac{2\pi}{N}kj\right)\right] \end{aligned} \tag{1}$$

This requires $O(N^2)$ operations.

The FFT is a DFT algorithm which reduces the computational complexity from $O(N^2)$ to $O(N \log_2 N)$. It is done by computing the 2-point DFT to generate a 4-point DFT and from a 4-point DFT to a 8-point, 16-point, ... 2^t-point DFT.

C. Shor's Algorithm

Given input $N(= p \times q)$, the Shor's algorithm consists of three steps: 1) period finding basedon number theory, 2) QFT speed up, and 3) calculate the factors based on the "period".

1) Greatest Common Divisor - GCD: To find gcd based on Euclidean algorithm:

```
def gcd(a, b):
    while b != 0:
        (a, b) = (b, a%b)
    return a
```

2) Period Finding: Factoring an integer may sound easy, as one can write a small program to do so. The issue is the time. When the number is big, the time needed to factor increase exponentially. Instead of factoring an integer a directly using brute force method, we can use an algorithm to find the order of an element a that is integer r such that

$$x^r \equiv 1 \mod N$$

that is

$$x^r - 1 \equiv 0 \mod N$$

To find the period r, we chose a random $x < n$. If r is even then use Euclidean algorithm to compute

$$x^r - 1 = \left(x^{\frac{r}{2}} - 1\right)\left(x^{\frac{r}{2}} + 1\right)$$

we get:

$$k_1 = \left(x^{\frac{r}{2}} - 1\right)$$

$$k_2 = \left(x^{\frac{r}{2}} + 1\right)$$

so

$$p, q = gcd\left(x^{\frac{r}{2}} \pm 1, N\right)$$

after factoring, we get

$$p = gcd(k_1, N),$$

$$q = gcd(k_2, N).$$

3) Shor's Quantum Integer Factoring: Shor's algorithm for period finding, an essential step for factoring integers, can be describes in the following steps:

a Randomly choose an integer a such that $0 < a < N$. Use the Euclidean algorithm to determine whether a and N are relatively prime.

b If not prime, use quantum parallelism to computer $f(x) = a^x \mod N$, for $x \in [0, 2^n - 1]$
choose

$$T = 2^n$$

where

$$N^2 \leq T \leq 2N^2$$

Initialize two registers of qubits, first an argument register with t qubits and second a function register with $n = \lceil \log_2 N \rceil$ bits. These registers start in the initial state:

$$|\psi_0\rangle = |0\rangle\,|0\rangle$$

c Apply a Hadamard gate on each of the quibit in the argument register to yield an equally weighted superposition of all integer from 0 to T:

$$|\psi_1\rangle = \frac{1}{\sqrt{T}} \sum_{a=0}^{T-1} |a\rangle\,|0\rangle$$

d Implement the modular expomentiation funcion $x^a \mod N$ on the function register, giving the state:

$$|\psi_2\rangle = \frac{1}{\sqrt{T}} \sum_{a=0} 0^{T-1} |a\rangle\,|x^a \mod N\rangle$$

e Perform a quantum Fourier transform on the argument register, resulting in the state:

$$|\psi_3\rangle = \frac{1}{\sqrt{T}} \sum_{a=0}^{T-1} \sum_{z=0}^{T-1} e^{(2\pi)(\frac{az}{r})} |Z\rangle |x^a \mod N\rangle$$

f Measurement. Wi2th the high probability, a value v close to a multiple of $\frac{2^n}{r}$

$$v = \frac{T}{r} = \frac{2^n}{r}$$

will be obtained, where q ranges from 0 to $r-1$.

g Find r using Euclid's algorithm With the measured v, the period can be calculated with

$$r = \frac{T}{v} = \frac{2^n}{v}.$$

Example: For $N = 21$, then $N^2 \leq T = 2^9 \leq 882(2N^2)$. Take $n = 9$, since $\lceil \log_2 N \rceil = 5$, the second register requires five qubits. Suppose random select $a = 11$ and the measurement of the second of the superposition produces $u = 8$. Suppose that measurement of the state return $v = 427$. Continue fraction to obtain a guess q for the period. Finally we get $q = 6$. Since 6 is even, $a^{6/2} - 1 = 11^3 - 1 = 1330$ and $a^{6/2} + 1 = 11^3 + 1 = 1332$, we then compute $gcd(21, 1330) = 7$ and $gcd(21, 1332) = 3$.

IV. Advancement in Shor's Algorithm

Quantum cryptoanalysis plays an important role in finding vulnerabilities of existing crypto systems. It can also become an effective tool in fighting adversaries in cyber operations. Efficient quantum algorithms are indispensable to the utilization of quantum computer resources to solve today's unsolvable problems [8]. It has the potential to break the current crypto systems such as RSA with the advances of next-generation quantum computers. Currently, most quantum cryptanalytic algorithms have limited capability to factor multiple integers due to the fact that each Quantum Fourier Transform, the speed machine to find out a period of a particular integer, requires a unique quantum circuit.

According to Shor's algorithm, once the period is found, finding factors (crypto keys) becomes easy. To break the RSA encryption, one needs to design a unique quantum circuit for each integer being exploited. Since there are a large number of integers to exploit, the current one integer-one circuit factor finding approach is not practically useful. The ongoing research is to discover techniques to automatically generate quantum circuits and factor multiple integers at once. Computational-wise, the aim is to speed up the cryptanalytic process by improving the order of approximation significantly on top of a polynomial degree that the QFT has saved from the unsolvable exponential degree.

A. Automatic Quantum Circuit Generation

It has been proofed that QFT is defined as a transformation between two quantum states that are determined using the values of FFT. If W is a Fourier matrix and $X = x_i$ and $Y = y_i$ are vectors such that $Y = WX$, then QFT is defined as the transformation

$$QFT\left(\sum_{k=0}^{N-1} x_k |k\rangle\right) = \sum_{k=0}^{N-1} y_k |k\rangle$$

Since QFT can be executed recursively, the calculation can be described as applying H gate and then apply $u1$ with $\pi/2$ rotation, then appy H gate again. The process repeat with every time rotating $1/2$ of the previous degree. The quantum then can be generated automatically.

B. Experiments

The initial experiments show that the assumption is correct. Using a quantum algorithm we developed, we were able to generate quantum circuits of 15, 21, 55, and 899 (29*31). The smaller numbers were able to pass the real quantum computers but the large number 899 were only able to be verified on a quantum simulator: *qasm_simulator*. The code was written in *Python* with IBM *qiskit* and *Jupiter Notebook* on a *Ubuntu 18.10 Cosmic 64* virtual machine running *Oracle Virtualbox*.

V. Conclusions and Further Discussions

Quantum mechanics has led to the discovery that considerable numbers of states can be manipulated at the same time thus significantly reduce the amount of time in processing. New quantum computers have shown the baseline of "quantum supremacy" in solving problems that classical digital computers practically cannot. Efficient quantum algorithms are key to enable computer scientists to take full advantage of the next generation of practical quantum computers to efficiently solve today's unsolvable problems. This research seeks to discover efficient quantum cryptologic methods (i.e. the art of revealing the secret) and secure quantum cryptographic techniques (i.e. the science of making the secret more secure).

In addition, the research plans to explore how artificial intelligence can assist in designing efficient quantum algorithms and test those algorithms using quantum simulators and on real quantum computers.

References

[1] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal of Computing*, pp. 1484 – 1509, 1997.

[2] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, M. P. de Almeida, A. Gilchrist, D. F. V. James, and A. G. White, "Photonic quantum computing: Shor's algorithm and the road to fault-tolerance," in *2008 Conference on Lasers and Electro-Optics and 2008 Conference on Quantum Electronics and Laser Science*, 2008, pp. 1–2.

[3] S. Wang. (2020, May) Quantum crypto and algorithms. [Online]. Available: http://pneumannsecurity.blogspot.com/2020/05/nsf-award-notice-for-award-quantum.html

[4] S. Wang, M. Rohde, and A. Ali, "Quantum cryptography and simulation: Tools and techniques," *Proc. of International Conference of Cryptography, Security and Privacy (ICCSP)*, pp. 36 – 41, 2020.

[5] P. Shor, "Process in quantum algorithms," *Quantum Information Processing*, pp. 5–13, 2004.

[6] M. A. Nielsen and I. L. Chuang, "Quantum computation and quantum information," *Cambridge University Press*, 2000.

[7] S. Wang and R. Ledley, "Modified neumann architecture with micro-os for security," in *CIICT*, 2007, pp. 303–310.

[8] C. Zalka, "Fast versions of shor's quantum factoring algorithm," *Quantum Physics*, pp. 1–37, 1998.