ANALYSIS OF THE CURRENT STATE OF QUANTUM COMPUTING AND APPLICATIONS TO WARFARE

A Dissertation
Presented to
The Academic Faculty

By

Jarrett Schultz

In Partial Fulfillment
of the Requirements for the Degree
Master's of Science in the
College of Computing
Center for Research into Novel Computing Hierarchies

Georgia Institute of Technology

May 2021

ANALYSIS OF THE CURRENT STATE OF QUANTUM COMPUTING AND APPLICATIONS TO WARFARE

Thesis committee:

Dr. Tom Conte
College of Computing
Georgia Institute of Technology

Dr. Margaret E. Kosal
Ivan Allen College of Liberal Arts
Georgia Institute of Technology

Date approved: April 30, 2021

ACKNOWLEDGMENTS

I would like to thank the members of my thesis committee for their help and guidance in the pursuit of my research – Tom Conte, who has inspired me to take an acute interest in low-level computing and architecture, Margaret Kosal, who has immersed me in a world of research that is new to me and has guided me throughout the process.

Special thanks to the friends and colleagues who made this work possible. Austin Adams for being a constant rock throughout the process and the rest of the members of CHAD who served as a valuable resource for exploration of my idea. Maya Neal who has coached me through the game of ultimate that serves as a much needed release. Shireen Budhwani who stuck around through long nights of work and never gave up staying up with me, even though sleep sometimes still came involuntarily.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ACRONYMS

C3 Command, Control and Communication

CMOS Complementary Metal-Oxide-Semiconductor

GPS Global Positioning System

JADC2 Joint All Domain Command and Control

MLS Maturity Likelihood Score

QPS Quantum Positioning System

RSA Rivest–Shamir–Adleman

SQUID Superconducting Quantum Interface Device

SUMMARY

The limitations imposed by the power wall provide the motivation for investigating non-traditional technologies such as quantum computing. It is garnering increased attention from all sectors, and development is picking up worldwide. This paper investigates 3 areas of quantum computing and its applications to warfare: Cryptography, Sensing, and Joint All Domain Command and Control. Analysis of current research, available prototypes and commercial products shows that there are novel techniques and significant improvement to classical alternatives. The specific applications analyzed have varied expected maturity dates ranging from within 5 years, within 10 years, to more than 20 years. These results indicate that quantum computing will be an important factor in the balance of power between the US and its adversaries in the coming years and that the state of quantum computing should be closely monitored.

CHAPTER 1
INTRODUCTION AND BACKGROUND

1.1 The Power Wall

Transistors are the fundamental basis of today's computing base. Virtually every computer, calculator, and electric powered device uses them. The most common type of transistor is called the Complementary Metal-Oxide-Semiconductor (CMOS). Driven by a massive consumer demand, these CMOS transistors have been developed over the years to become smaller, faster, and more reliable. In turn, the devices they power have reaped the benefits. While the CMOS manufacturers continue to make smaller transistors every year, the usefulness of a smaller transistor has been trumped by a fourth aspect: heat generation.

CMOS computers have a central processing unit, or CPU, which accomplishes most of the work that needs to be done in a computer. One can view the CPU as divided into functional units, where each can accomplish a single task. The CPU has many functional units that each accomplish one task per cycle, which is the smallest unit of work. If we have a single functional unit, we can accomplish one task per cycle. If we increase this to five functional units, we can accomplish 5 tasks per cycle. In a technical sense, making a computer faster refers to increasing the number of tasks completed per cycle.

To make a computer faster, we have several options. First, we can reduce the time needed to complete a cycle. Reducing cycle time means making each functional unit faster so we can increase the frequency of cycles. This is commonly referred to as increasing the frequency of a CPU and is the result of either better transistors or simpler functional units. Secondly, we can add more functional units to allow for more concurrent task completion. Lastly, we can employ architecture tricks to make the functional units complete tasks faster, at the expense of increasing the number of transistors.

For years, the computer industry has seen sizable performance improvements purely by relying on better transistors each year to increase the frequency of CPUs. In 2005, we hit what is called “the power wall”. While transistors were able to handle higher frequencies, they began generating so much heat that it would compromise the integrity of the CPU. The bottleneck had now shifted to heat management and the industry was beginning to move toward option two - adding functional units.

The industry began adding more functional units which helped spread out the heat generation. These additional functional units are marketed as “cores” and allow tasks to be completed concurrently. However, these cores have to talk to each other and inherently incur some kind of overhead. This overhead means that while two cores may be able to complete twice the number of tasks, some of these tasks will be specifically dedicated to overhead and can reduce the visible improvement to less than the amount of real work that two cores can accomplish. As more cores are added, the overhead is increased, and the perceived benefit is reduced asymptotically. When the improvements began dwindling, the industry then turned to the final option: architectural tricks.

Architectural tricks were initially very useful, with advancements in the technology initially providing large improvements. However, these advancements began to yield smaller and smaller increases in speed, and thus are becoming less useful. Now that improvements in speed are slowing, the end of optimization for CMOS computing seems to be in sight.

Industry and the world as a whole are now turning to alternatives to CMOS computing. They seek to change how computing devices fundamentally work by replacing the traditional transistor approach entirely. One such promising alternative is quantum computing which this paper seeks to investigate.

1.2 Basics of Quantum Computing

CMOS computing operates on the fundamental concept of a bit. A bit can hold a value of on or off, typically referred to as 0 or 1. Using this as a baseline, we can convert a series

of ones and zeroes using a series of tasks to provide another series of ones and zeroes that holds some meaning to the operator. Quantum computing challenges this concept by operating on the fundamental concept of a quantum bit, or qubit.

While drastically simplified, we can view a qubit as being combination of percent chances to be 0 or 1. For instance, a qubit can be $< 40, 60 >$ which would represent a superposition such that 40% of being a 0 and 60% chance of being a 1. A fundamental property of these qubits is that measuring the qubit collapses this vector into 0 or 1. In other words, if we measure a qubit to be 0, then the vector that represents that qubit is mutated and becomes $< 100, 0 >$. At its core, quantum computing works by manipulating many qubits into a specific superposition in order to measure its outcome on a statistical basis.

Quantum computers are useful because they see a much quicker runtimes on a particular set of problems, named bounded-error quantum polynomial time problems. Since quantum computers are only useful for computing this specific set of problems, they will likely be implemented as a "plug-in" to a classical computer. Classical computers will outsource these bounded-error quantum polynomial time problems to the quantum computer and perform the rest of the tasks.

1.3 State of Quantum Computing

Just as classical computers have a CPU and a GPU, quantum computers are developing in a similar fashion with universal gate and quantum annealing quantum computers, respectively. This paper focuses on the general progress quantum computing and will thus restrict the discussion to that of universal gate quantum computers.

Quantum advantage, or quantum supremacy, refers to proof that quantum computers can successfully perform a computation orders of magnitude more efficiently than a classical computer. Google has recently put forth an experiment that they claim demonstrates this quantum advantage [1]. While contested in the quantum community, it is an important

step in the development of quantum computers.

Current universal gate quantum computers have less than 100 qubits [1, 2]. To have a quantum computer run a realistic version of quantum algorithms, it will need millions or even billions of qubits. One paper, which proposes a construction of a quantum computer to factor large integers using Shor's algorithm stated that it would require 20 million qubits [3].

1.4 Research Questions

This paper will choose three areas of quantum computing in order to investigate the following research questions:

1. How distant is the realization of these quantum technologies?
2. What effect, if any, does each area of quantum computing have in shifting the power balance of the US and its adversaries?

To address these research questions, this paper will be organized as follows. Chapter 2 will discuss the methodology for answering the research questions. Chapters 3, 4, and 5 will discuss Cryptography, Sensing, Joint All Domain Command and Control (JADC2), respectively. Chapter 6 will provide any conclusions and recommendations as well as avenues for future work.

CHAPTER 2

METHODOLOGY

This work will assign two scores: Maturity Likelihood Score (MLS) and Improvement Score to help provide insight in each area of quantum computing. The following tables show the possible values for each score.

Table 2.1: MLS values

MLS Score	Meaning
1	5 years
2	10 years
3	20+ years

Table 2.2: MLS values

Improvement Score	Meaning
1	Transforming Technique
2	Improvements, but not novel
3	Little change

2.1 MLS and Improvement Score

In an effort to answer the aforementioned research questions, this paper will assign two scores to each of three areas of quantum computing. The first score is the Maturity Likelihood Score (MLS) and is shown in Table 2.1. This score represents the likely time until a mature version of the technology is able to be used in its professed role. Scores of 1, 2, and 3 are possible. These scores represent likely maturity within 5 years, 10 years, or 20+ years, respectively. This score will be a result of the combination of recent public research, existence of prototypes, and commercial products. The second score is the Improvement Score which is shown in Table 2.2 and is meant to convey the degree to which the quantum technology improves upon its classical predecessor. Scores of 1, 2, and 3 are possible.

These scores represent a transforming technique, major improvements, and little change, respectively. The Improvement Score will be a descriptive analysis of the specific improvements that the technology has over its predecessor. Aspects that will be used for this score include accuracy, size, efficiency and confidentiality.

For example, suppose an application has an MLS score of 1 and an Improvement Score of 2. This application would have working prototypes, large amounts of scientific research and likely some business ventures. It would see significant improvements upon the predecessor technology, but no major disruption in the application paradigm.

2.2 Overall Area Calculation

Multiple applications are explored within each area and are assigned their own unique scores. Then, the scores will be aggregated to score the area as a whole. To calculate an aggregate score, the median is taken of all applications. If there are multiple medians, then the middle score of 2 is chosen which is then representative of the average. The aggregate scores for each area will be analyzed at the end of the paper with the intent to illustrate the current state of quantum computing and the likely impact that quantum technologies will have on the balance of the power between the US and its adversaries.

CHAPTER 3
CRYPTOGRAPHY

Breach of communications can be disastrous for a wartime operation [4]. In Cryptography, quantum computing can leverage quantum entanglement and superposition to make sure that communications are secure in the presence of adversaries. This paper looks at three key applications: Shor's algorithm, quantum key distribution, and mistrustful communication.

3.1 Shor's Algorithm

The most prevalent modern day encryption algorithm, Rivest–Shamir–Adleman (RSA), relies on the premise that there is no efficient way to factor large integers. This algorithm is the cornerstone of almost all modern-day communications and to break it would turn the internet into a sort of wild west which garners heavy media attention. Shor's algorithm shows that factoring large integers can be efficient on quantum computers [5], effectively breaking RSA.

Shor's algorithm shows that it can break RSA, but the realization of a quantum computer with enough qubits to run the algorithm is likely distant [3]. The NSA, NIST, and the scientific community has been taking steps since 2016 to create a quantum resistant algorithm [6, 7] and to mitigate the effects of this quantum breakdown of RSA. These algorithms will rely on a unique mathematical premise that is not known to be efficiently solvable by quantum computers and will theoretically be secure even in the quantum age.

The efforts to find a replacement for RSA will likely be successful and will squander any tangible benefit from running Shor's algorithm. For this reason, it is noted in this paper that Shor's algorithm is not known to have a significant impact or use in warfare.

3.2 Quantum Key Distribution

In classical cryptographic systems such as RSA, a secret key is shared between two parties wishing to communicate. This key is used to encrypt a message from one party which is then transmitted by public means to the other party. Since this message is passed over a public space, any attentive listener can read the encrypted message. However, the attacker cannot decrypt the message without knowledge of the secret key previously transmitted between the two parties. Transmission of this key is integral to maintaining the secrecy of the message. Quantum key distribution (QKD) puts forth a way to distribute this key with a unique property so it can detect if a third party is attempting to gain knowledge of it.

Experimental implementations of QKD have been around for many years dating back to at least 2006 [8]. These implementations are limited in scale and are primarily used to show improvements in technique and hardware. There also exist several commercial ventures offering QKD systems, showing that there may be significant interest in commercial development. This points to interest in developing QKD as well as significant progress in making a system that can be implemented on a more widespread basis. However, development is needed before the rigor and precision that is needed for military applications is met.

The usefulness of QKD is unclear since it still relies on classical cryptography and solves a problem where classical cryptography already provides security. Still, it is important to note that QKD provides a provably secure communication, which a classical cryptographic algorithm cannot provide. Development of this technique may be fruitful for use with communications that require a great deal of discretion.

3.3 Mistrustful Communication

Mistrustful cryptography allows two parties to enter communication when they do not trust each other. The immediate application allows an unverifiable party to communicate with

the US and provides avenues of communication for secret operations and recovery of lost assets. This system cannot achieve unconditional security like QKD but can provide security against quantum attacks much like classical algorithms are able to provide security from classical computers.

There exists a proposal for this technique which holds promise [9], but there have yet to be any prototypes or related business ventures. Of the three applications, this one has been the least developed and the maturity of it is likely very far into the future.

3.4 Takeaways

Table 3.1 shows the MLS and Improvement Score for each application and the average rounded score for cryptography.

Table 3.1: MLS and Improvement Score for cryptography applications

Application	MLS	Improvement Score
Shor's Algorithm	3	3
QKD	1	2
Mistrustful Communication	3	1
Cryptography	3	2

Cryptography has scored an MLS of 3 and an Improvement Score of 2. QKD was the only application with the presence of prototypes and business units. The Improvement Scores for these applications varied significantly and has thus received a score of 2, showing improvement over existing techniques. These applications see some promise, but not enough progress to warrant attention until more is learned about the usefulness of the technologies.

CHAPTER 4

SENSING

The US Defense Task Force has identified quantum computing as an important resource to remain competitive [10]. Additionally, the DoD has found that quantum sensors can outperform current sensors and that they "offer the potential for dramatically improved performance for critical DoD missions" [11]. This paper discusses three important applications of quantum sensing: positioning, clocks, and magnetometers.

4.1 Positioning

4.1.1 Active

There is a great civilian and military reliance on Global Positioning System (GPS) for active positioning. Some Quantum Positioning System (QPS)s introduce an alternative to GPS that still relies on satellites, but no longer uses electromagnetic waves. Importantly, this provides an avenue to more effectively avoid interference and improve the accuracy [12]. Another proposal [13] presents a system that can work in multiple modes, some no longer relying on satellite communication. The benefits of such a system are evident in adversarial environments. While a QPS promises large improvements in accuracy, no prototypes currently exist. Such a system relies on host of different quantum sensors [12], some of which are not feasible to meet requirements yet.

4.1.2 Passive

Passive positioning is often used to enhance or replace GPS. A passive QPS is also similar to the classical system, except that it promises greatly improved accuracy [12]. One component of the system is the quantum gyroscope, which relies on quantum entanglement.

Quantum entanglement is still something that researchers are working to understand and the development of these sensors require much more time. Because of this, the development of a passive QPS will likely be more delayed than its active counterpart. However, a classical passive positioning system can be used in its place with an active QPS to achieve the benefits of the active system.

4.2 Clocks

Quantum clocks boast huge improvements in accuracy, with prototypes such as the NIST-F2 being accurate to the second for 300 million years [14]. Other quantum clocks are orders of magnitude smaller or consume much less energy. One chip-scale atomic clock presents a prototype that takes up a volume of less than $1cm^3$ [15] while consuming less energy than the classical approach.

With the warfighting system becoming increasingly dependent on electronic means, the benefits of greater accuracy and smaller size are evident. Prototypes exist for these kinds of clocks and the development of further prototypes with increased durability are likely in the near term.

4.3 Magnetometers

Magnetometers are by definition able to measure electronic waves. One application of this technology is called a Superconducting Quantum Interface Device (SQUID) and is able to detect submarines at a range of 6km [16]. For comparison, one modern classical method which involves a network of sensors can detect submarines with a square kilometer. These SQUIDs provide a huge improvement in places such as the South China Sea, where China hopes to gain full control [17].

There exists research for a prototype [18] of a SQUID. Research for such a technology dates back to at least 1989 [19], indicating that such sensors are currently practical and a successful prototype may be achieved in the near future.

4.4 Takeaways

Quantum sensors show improvements in accuracy, anti-tampering ability, size, and effectiveness over classical methods. With many prototypes already available, the maturity of this technology seems to be very short term and the applications of many of the technologies are evident in an adversarial environment. Referring to Table 4.1, this paper present a near-term MLS and significant Improvement Score.

Table 4.1: MLS and Improvement Score for cryptography applications

Application	MLS	Improvement Score
Positioning	1	1
Clocks	1	2
Magnetometers	1	1
Sensors	1	1

CHAPTER 5
JOINT ALL DOMAIN COMMAND AND CONTROL

JADC2 is part of a larger effort by the DoD to modernize and integrate the current Command, Control and Communication (C3) systems [20]. This effort attempts to provide a means of command delivery that will provide clarity, accuracy, and effectiveness to adversarial environments. It will rely on development of new technologies and enhancement of existing systems. As this chapter will discuss, quantum puts forth a variety of technologies that will improve several aspects of the system.

5.1 Advanced Positioning and Timing

One of the primary goals of the C3 modernization strategy is to enhance all aspects of Advanced Positioning and Timing (AP&T). As discussed in chapter 4, quantum technology brings a host of improvements to classical sensors that will increase accuracy, decrease size, and provide alternative methods of delivery.

The maturity of these technologies received an overall score of 1, indicating maturity within 5 years. Additional investment will be need to integrate these systems into the larger ecosystem, but the overall development time may remain largely similar. Thus, this aspect of JADC2 promises novel improvements and likely availability within 5 years.

5.2 Secure Communication

To have an effective distribution of command, commands and general communications must be kept from adversaries. The potentially devastating effects of a breach of this secrecy was studied in great detail during the Vietnam War [4]. As discussed in chapter 3, quantum technology provides provably secure communication through QKD and avenues

for mistrustful communication. The physical technology, however, is currently underdeveloped and additional research will be needed to mature these technologies and integrate them into the larger JADC2 ecosystem.

5.3 Database Searching

JADC2 is likely going to be a large distributed system where latency matters. In such a large system, accesses to databases that contain large amounts of information will be an important part of the overall system. Quantum computing has a useful technique by the name of Grover's algorithm that allows a more efficient search of large databases [21].

In an unordered database with n elements, a search through the database will on average have to traverse through $n/2$ elements. Grover's algorithm reduces this search to $\sqrt{n}$, making this a significant improvement in databases that contain a large amount of elements. However, modern day implementations of Grover's algorithm are limited to less than 10 qubits [22] when dozens, thousands or possibly million of qubits are needed to run Grover's algorithm on a large database.

5.4 Takeaways

JADC2 has been identified as an integral part of future American national security. Quantum technology presents greater accuracy in positioning tools, more secure communication, and improved database search times. Referring to Table 5.1, we can see how this affects the overall MLS and Improvement Score.

Table 5.1: MLS and Improvement Score for JADC2 applications

Application	MLS	Improvement Score
AP&T	1	1
Secure Communication	3	1
Database Searching	2	2
JADC2	2	1

Notably, the overall Improvement Score is very high. This indicates that these technologies will be important to maintaining an edge in warfare.

CHAPTER 6

CONCLUSIONS AND RECOMMENDATIONS

6.1 Conclusions and Future Direction

The analysis found that each area of quantum computing has significant improvements over classical alternatives and have potential to greatly affect the balance of power. However, there is great diversity among the MLS scores which indicates that quantum computing is still young and will require many more years of development and research. Cryptography is far from seeing field use, but quantum sensors will be ready relatively soon. Lastly, quantum technology has significant impact in improving C2 which is a key DoD objective [20].

Table 6.1: MLS and Improvement Score for all areas

Area	MLS	Improvement Score
Cryptography	3	2
Sensing	1	1
JADC2	2	1

There is still further research to be done in ensuring the reproducibility of the scores. One method of constraining these definitions is through analysis of past technologies that have been subsequently adopted. Quantum computing is a vast field that begs further investigation and this paper may serve as a launching point for additional quantum technologies with military promise. Additionally, an in-depth comparison of each quantum technology to its classical alternative may prove fruitful.

6.2 Recommendations

The DoD has noted the importance of quantum computing [11] and the results of this study agree. Many of the specific quantum technologies in this paper show promise and other countries have recognized this as well. This paper indicates that further investigation into these technologies may be important to maintaining a military edge in future operations and a close monitoring of other countries may be advisable.

REFERENCES

[1] F. Arute, K. Arya, R. Babbush, *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, pp. 505–510, 2019, doi:10.1038/s41586-019-1666-5.

[2] G. Zhu and A. Cross, "Hardware-aware approach for fault-tolerant quantum computation," *Physical Review X*, 2020.

[3] C. Gidney and M. Ekera, "How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits," *Quantum 5*, vol. 433, 2021, doi:10.22331/q-2021-04-15-433.

[4] D. G. Boak, "A history of u.s. communications security (u)," *The David G. Boak Lectures*, vol. 2, 1981.

[5] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum processor," *SIAM J.Sci.Statist.Comput.*, vol. 1484, 1996, doi:10.1137/S009753979529

[6] A. Mandviwalla, K. Ohshiro, and B. Ji, "Implementing grover's algorithm on the ibm quantum computers," in *2018 IEEE International Conference on Big Data (Big Data)*, 2018, pp. 2531–2537.

[7] NSA, "Post-quantum cybersecurity resources," 2021.

[8] P. A. Hiskett *et al.*, "Long-distance quantum key distribution in optical fibre," *New J. Phys.*, vol. 8, no. 193, 2006, doi:10.1137/S0097539795293172.

[9] A. kent, "A proposal for founding mistrustful quantum cryptography on coin tossing," *Phys. Rev. A*, vol. 68, 2003.

[10] S. Moulton, J. Banks, *et al.*, "Future of defense task force report 2020," *Future of Defense Task Force*, 2020.

[11] J. Manferdelli and R. Wisnieff, "Application of quantum technologies," *Future of Defense Task Force*, 2019.

[12] D. Feng, "Review of quantum navigation," *ICAESEE*, vol. 237, 2019, doi:10.1103/PhysRevA.68.012

[13] T. Bahder, "Quantum positioning system," 2004.

[14] T. Heavner *et al.*, "First accuracy evaluation of nist-f2," *Metrologia*, vol. 51, no. 3, 2014.

[15] R. Lutwak, J. Deng, W. Riley, *et al.*, "The chip-scale atomic clock - low-power physics package,"

[16] S. Terlizzi, "The challenge of advanced weapons to us-russia strategic stability," 2018, Chapter 3.

[17] D. Hambling, "China's quantum submarine detector could seal south china sea," *NewScientist*, 2017.

[18] G. Zhang *et al.*, "Practical dc squid system: Devices and electronics," *Physica C: Superconductivity and its applications*, vol. 518, 2015.

[19] P. M. Moser, "Gravitational detection of submarines," 1989.

[20] D. Norquist, "Dod c3 modernization strategy,"

[21] A. Mandviwalla, K. Ohshiro, B. Ji, *et al.*, "Implementing grover's algorithm on the ibm quantum computers," *2018 IEEE International Conference on Big Data (Big Data)*, 2018.

[22] V. B. Karlsson and P. Stromberg, "4-qubit grover's algorithm implemented for the ibmqx5 architecture," 2018.