# Analysis of the Potential Benefits from Using Quantum Computing for Aerospace Applications


**Dominic Rosch-Grace**
**Department of Computer Science**
**North Dakota State University**
**1320 Albrecht Blvd., Room 258**
**Fargo, ND 58102**
**dominic.rosch@ndsu.edu**

**Jeremy Straub**
**Department of Computer Science**
**North Dakota State University**
**1320 Albrecht Blvd., Room 258**
**Fargo, ND 58102**
**jeremy.straub@ndsu.edu**



*Abstract*—**This paper discusses the benefits that can be enjoyed from the possible applications of quantum computing to the aerospace sector. It discusses these benefits for various tasks and applications such as artificial intelligence, key distribution and simulation. The challenge of determining what aerospace applications will be best allocated to quantum devices is also discussed. The method for best utilizing quantum computing for aerospace applications is also considered and the benefits of a grid-based implementation of computational resources are discussed. A collection of network-connected heterogenous devices could be used to support the effective use of computational resources. It could be used for the operations and development of simulations as well as machine learning and other software applications. This paper also presents a summary of potential use-cases, as well as a discussion of the work necessary to expedite the process of quantum computing development.**


## TABLE OF CONTENTS


1. INTRODUCTION ........................................................ 1
2. INTRODUCTION TO QUANTUM COMPUTING......... 2
3. QUANTUM SIMULATION FOR AEROSPACE ............ 3
4. QUANTUM AEROSPACE WITH GRID COMPUTING.. 3
5. QUANTUM KEY DISTRIBUTION AND QUANTUM ARTIFICIAL INTELLIGENCE FOR AEROSPACE AUTONOMY ................................................................ 3
6. QUANTUM SIMULATION AND COMPOUND QUANTUM COMPUTING ADVANCEMENTS.................. 4
7. IMPLICATIONS AND FUTURE WORK....................... 4
8. CONCLUSION........................................................... 5
ACKNOWLEDGEMENTS .............................................. 5
REFERENCES.............................................................. 5
BIOGRAPHY ............................................................... 6


## 1. INTRODUCTION

Quantum computing is poised to provide a variety of benefits for complex simulation tasks. By virtue of the inherent random of quantum bits and the perceived efficacy of some quantum algorithms, certain computing processes, through quantum simulation, may be expedited to facilitate more accuracy in otherwise computationally expensive aerospace simulations. Prior work has described the capability of quantum computing simulation for numerous areas of scientific research, such as chemistry [1], pharmaceutical development [2], and advancements in materials science [3], to name a few. These areas of research are recognizably well-suited to quantum computing simulation, as key advancements in the aforementioned areas are dependent on understanding their underlying mechanics at the microscale. In considering this, advancements in aerospace simulation and design may also exploit the simulation capabilities of quantum computers, as certain characteristics such as fluid dynamics in simulation and advancements in materials science for aerospace design require an understanding of their respective microscale mechanics.

Quantum key distribution is among the most promising approaches to realizing quantum computing practicality. Here, the possibility of developing and implementing quantum cryptographic frameworks to secure aerospace systems is considered. At present, there is a degree of concern over the potential for prime-factor-finding capability of quantum computing systems [4]. The difficulty in identifying these prime factors serves as the basis for common encryption methodologies, such as RSA. Quantum key distribution is a potential approach to alleviating these concerns, as quantum computers are poised to threaten RSA encryption [5].

Similarly, quantum artificial intelligence is another prospective application for capable quantum computers. Here, the possibility of exploiting the parallel nature of quantum computations for machine learning applications is discussed, as well as the possibility of their integration into aerospace systems. Quantum artificial intelligence has demonstrated its capability in expediting certain machine learning applications [6]. Disregarding the current hardware and software challenges quantum computing development is facing, recent quantum machine learning algorithms have demonstrated a variety of key possibilities in the utilization of quantum computing systems for machine learning applications [7].

Figure 1 illustrates the potential benefits quantum computing can offer the field of aerospace. As shown, implementations

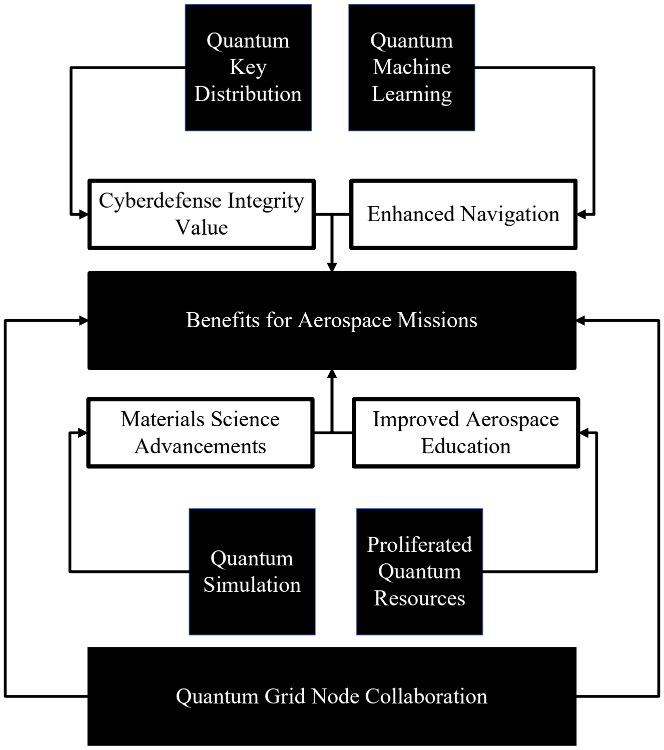


**Figure 1. Quantum Computing Benefits for Aerospace.**

of quantum key distribution can be utilized to strengthen the cyber-integrity of aerospace systems connected over a network. This effectively reinforces the cyber-defense of this asset, ensuring that third-party access to sensitive information regarding it is impractical to achieve.

Quantum machine learning has the potential to offer a variety of benefits for path-finding situations. In this arbitrary implementation, quantum computing systems can be considered for checking a variety of routes concurrently, effectively decreasing computing time costs.

Quantum simulation acts as the foundation for advancements in materials science. Here, this diagram follows the assumption that quantum simulation was utilized to develop a material that was utilized in the construction of the aircraft.

The proliferation of quantum resources node depicts the contribution of large-scale recognition of quantum capability and how it could ultimately strengthen the education landscape, producing more capable aerospace-oriented individuals, as well as providing faculty with the resources to tend towards new ideas.

Finally, the collaborative capability of a quantum grid environment facilitates communication between nodes connected over a network. This situation is not unlike the computational cloud, in that computational resources, in this scenario, have the potential to share a variety of programs regardless of location, so long as these devices maintain a network connection.

This paper continues with a brief introduction to quantum computing in Section 2. Sections 3 and 4 talk about quantum computing simulation and grid computing for aerospace applications, respectively. Section 5 discusses the use of quantum key distribution and quantum computing artificial intelligence uses. Section 6 discusses quantum computing simulation. Section 7 discusses the implications of the previous section and the needed future work, before the paper concludes in Section 8.

## 2. Introduction to Quantum Computing

Quantum computing is a relatively new approach to computing machinery that exploits concepts of quantum mechanics for computational processing. Here, quantum superposition and entanglement serve as the basis for quantum computing prowess for rapidly performing certain tasks, such as factoring large integers [8]. The elementary unit of information utilized in quantum computers is the quantum bit or qubit. The qubit can be visualized as a Bloch sphere [9] where its information can be determined by traits such as an upwards or downwards spin for electron implementations of qubits, or polarization for photon implementations of qubits.

The applicability of qubits for measurements on quantum systems is derived from the inherent uncertainty of the instantaneous quantum state of the qubit. That is, qubits can be mathematically described as a superposition of all possible states within the quantum system, where the probability of measuring the qubit in one of the states is based on its respective amplitude of the state squared.

Superposition of qubits is not unlike a coin spinning in the air after flipping it. Here, the possibility of measuring the coin in heads or tails after it lands is 50/50. As the coin is spinning, it assumes a "superposition" of both heads and tails, where having the coin land and observing whether it is heads or tails is analogous to measuring the qubit. Here, observing the coin is similar to measuring the quantum state of a qubit and having its wave function "collapse." When a quantum state collapses, it rids itself of the uncertainty factor and assumes one of the possible states.

Advancements in the field of quantum computing are measured by a variety of factors. At present, quantum decoherence maintains its spot as a considerable obstacle in the realization of large-scale quantum computing systems, further necessitating the need for quantum error correction [10]. Similarly, a variety of potential use-cases of quantum computers are dependent on a certain number of logical qubits. For example, a proper implementation of Shor's prime integer factorization algorithm [8] would require significantly more qubits than are available at present to be viable.

Regarding benefits of quantum computers, the inherent capability of quantum computing systems for certain tasks, as discussed, is in the uncertainty factor of qubits utilized for calculations. Here, quantum computers can effectively accomplish a variety of tasks concurrently, as opposed to modern digital computers that follow a sequential/round-robin approach to processing tasks. Another significant benefit of quantum computers is their capability to generate true random integer values [11]. To differentiate, digital computers generate random integers based on a seed value that lacks genuine random, effectively rendering them less effective for tasks that require generation of random values.

The true capabilities of a quantum computing machinery, at present, are not fully understood. The quantum computing research landscape is heavily focused on the mitigation of quantum decoherence rates, as well as approaches to integrating more qubits into their systems. Alternatively, a short-term consideration that effectively sparked the necessity for quantum computing capacity development was the capability of quantum systems to potentially render RSA encryption obsolete [5]. As the potential applications of quantum computers were further understood, a variety of proposals became evident, reinforcing the possible capability of quantum computers for future endeavors.

## 3. QUANTUM SIMULATION FOR AEROSPACE

Quantum computing for simulation is a relatively new, yet approach to scientific development for a variety of different research areas [12]. A considerable problem with modern digital simulation is that certain processes that need to be simulated can be computationally demanding and require more resources than are available. A benefit of harnessing quantum computing systems for simulation is evident in the application of quantum algorithms for certain tasks. Here, some computations can be processed concurrently, that is, quantum simulation is parallel by nature [13]. This has the potential to expedite certain computationally expensive processes, the likes of which may exist in modern simulation methodologies for aerospace.

An example of some aerospace simulation characteristics that may benefit from quantum simulation is in simulating fluid mechanics of aerodynamics. Mathematical modeling is a key element of aerodynamics modeling that has an inherent compromise factor [14], in that the mathematical complexity of all factors considered in a simulation environment is computationally expensive to effectively analyze and apply, where simulation accuracy and cost have an intrinsic trade-off. This may potentially be alleviated by applying quantum simulators, where properties of the natural world to be simulated use quantum mechanics as a basis for their operations. In essence, this follows the idea that a collection of fundamental particles, such as a fluid to be simulated for aerospace simulation, would be best facilitated by the quantum mechanics utilized in quantum computers, as opposed to the binary mechanics of digital computing machinery.

Conversely, a variety of presently required simulation scenarios are classically intractable, further reinforcing the necessity for quantum computing simulation capability. It is speculated that not only would a quantum computing simulator render high complexity quantum mechanical simulation processes possible, but also boast an exponential speedup over classical systems [15]. This presents a variety of potential resultant benefits, as this notion posits that otherwise intractable simulation requirements could be facilitated/expedited on quantum computing simulation systems. Further, simulation of chemical reactions by virtue of ideal quantum computing systems may facilitate a cascade of advancements in materials science. A potential byproduct of this would be in the discovery of a new lightweight, cost-effective material for aerospace engineering applications.

Education is another key possibility for leveraging quantum-enhanced simulation capabilities. Aerospace education is dependent on certain simulation software to train prospective pilots to operate air and space vehicles, among other things [16], [17]. With improved accuracy and the potential for enhanced computing power for quantum computing pilot simulation software, aerospace students are effectively receiving a more accurate educational simulation environment. Likewise, these students and faculty may also contribute to the development of aerospace design, as these resources could be given to them upon quantum computing proliferation.

## 4. QUANTUM AEROSPACE WITH GRID COMPUTING

In a large-scale computing environment, a significant problem in maintaining stability is the management of data marshalling [18] and task allocation. A quantum computing grid-based infrastructure should be considered for the heterogeneous nature of computing grids, as well as their task scheduling capability. With this, previously implemented task classification algorithms for grid environments could be modified to identify what tasks would be best allocated to quantum computing systems within the grid. In essence, a realized implementation of the aforementioned would effectively facilitate a collaborative network environment, where all devices connected over this grid effectively communicate with each other. The scheduling system would serve as the moderator over the grid network traffic and task allocation, considering a computing task, as well as what devices are best suited for it/available. Not only would this provide a variety of communication benefits, but a grid implementation also boasts resource distribution capabilities.

## 5. QUANTUM KEY DISTRIBUTION AND QUANTUM ARTIFICIAL INTELLIGENCE FOR AEROSPACE AUTONOMY

The advent of quantum computing capability presented a number of key logistical challenges for currently implemented cyber-defense frameworks. At present, there are a variety of concerns over the potential for quantum computing systems to render common encryption methodologies, such as RSA encryption, obsolete [4]. In response to this, quantum key distribution is a considerable area of research that has not only stressed the necessity for innovative, quantum-capable encryption techniques, but has also presented a variety of similar innovations in response to this [19]. Further, many cyber-physical assets, such as aerospace vehicles, are dependent on the security of their computational network environment. Here, the fear of potentially encryption-breaking quantum computers may be alleviated if these aerospace vehicles are equipped with quantum-resistant encryption techniques based on quantum key distribution.

A significantly impactful area within the quantum computing research landscape is the potential for quantum algorithms to be utilized for machine learning optimization applications. A variety of machine learning processes have been speculated to be expedited by certain quantum computing machine learning algorithms. At present, most data analysis and machine learning implementations are heavily dependent on executing matrix operations on vectors within a high-dimensional vector space [6]. Similarly, matrix operations also serve as the basis for the mathematics behind quantum mechanics, demonstrating the possibility of applying the quantum mechanical principles of quantum computers to modern machine learning implementations. Empirically, machine learning approaches such as deep neural networks play a key role in the development of autonomous vehicles [20], implying the capability of similar applications, in tandem with the optimization potential of quantum computers for aerospace implementations of autonomous vehicles.

## 6. QUANTUM SIMULATION AND COMPOUND QUANTUM COMPUTING ADVANCEMENTS

As quantum computing is, at present, significantly impeded by a variety of key logistical challenges such as qubit decoherence [21], harnessing quantum simulation for research in quantum computing is another possible use-case. In this scenario, quantum simulation is applied to simulate and understand the underlying mechanics of current quantum computers, where qubits and their environment are faced with a variety of different environmental scenarios to test for efficacy.

Figure 2 illustrates the aforementioned cycle. Here, the process begins by executing a module of quantum computing simulations, where the left node within the quantum simulation timeframe denotes environmental/qubit experimentation. The right node represents a prospective software implementation for this sprint of quantum simulation. After the simulation run, the results are analyzed and potential advancements in quantum computing technology are recorded. In this instance, advancements refers to both potential applications and a greater degree of understanding of quantum computing mechanics. These advancements are then used to improve upon existing quantum computing simulation implementations. As a cyclic process, an additional quantum simulation run would be necessary, where the previously mentioned processes following the timeframe are then executed. Here, the process effectively cascades into a plethora of quantum computing technological advancements resulting from greater understanding of/improvements upon existing quantum computing principles or technology. The basis for this scenario is the idea that the best way to simulate quantum mechanics is with machinery that exploits the same mechanics for their computations, i.e., a quantum computer. Here, the quantum mechanics that dictates the operations of quantum computing machinery are simulated, resulting in advancements in quantum computing technology.

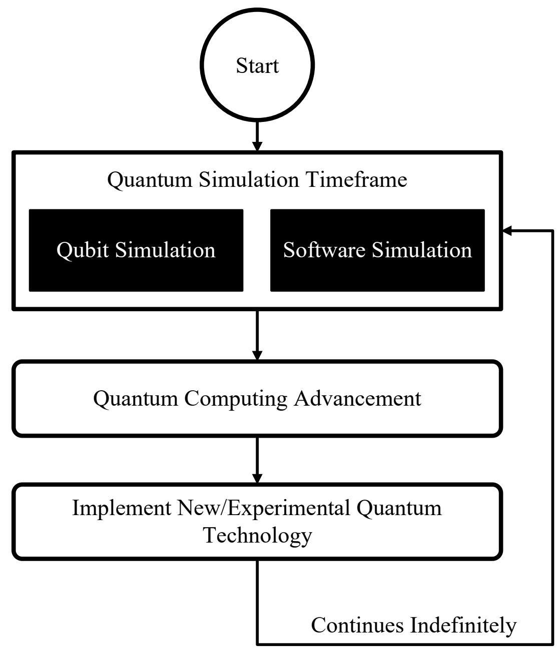


**Figure 2. Compounding Quantum Computing Advancements from Simulation.**

## 7. IMPLICATIONS AND FUTURE WORK

At present, scalable quantum computing systems are limited by a variety of factors. Among the most prominent of challenges is the decoherence rates of qubits [21]. Here, the overall instability of qubits presents key logistical challenges in quantum error correction and hardware improvements. Many quantum computers need to be kept at significantly low temperatures, increasing the computational cost, and lowering the practicality of proliferation of this quantum hardware. If quantum computing hardware were to be implemented in cyber-physical aerospace systems, advancements in room temperature quantum computing for qubit stability is necessary. Likewise, quantum error correction needs significant consideration in both mitigating/compensating for qubit decoherence rates and scalability improvements for when more qubits are to be added to future quantum computers. This is particularly important, as many potentially applicable quantum algorithms are dependent on a number of logical qubits significantly beyond the present qubit count.

Quantum computing machinery is a considerably rare resource as a tool for research and education. Proliferation of quantum computing hardware would play a significant role in the long-term capability of quantum computing systems, as getting this capability in that hands of consumers/research organizations would increase the level of national exposure to the concepts and applications. Likewise, national recognition of quantum software development may ultimately serve as the foundation for the creation of quantum software development curriculums in modern educational institutions. A greater amount of quantum computing researchers has the potential to expedite quantum computing advancements, as there would consequentially be more ideas and developments in circulation.

More resources in the research landscape should also be focused on increasing the current logical qubit count, as well as a mitigation of quantum noise for more long-term processing capability. At present, qubits tend to produce erroneous outputs in their calculations as a consequence of quantum decoherence, effectively halting the implementation of higher-qubit quantum computing systems, as well as the long-term realization of large-scale quantum computing resources.

The miniaturization of quantum computing hardware is also a significant challenge currently being faced in the quantum computing research landscape. As mentioned previously, quantum computers require significant cooling to assist in the maintenance of stable qubits for calculations. This tends to take up significant space, as well as cost. Inclusion of quantum computing hardware into cyber-physical assets is dependent on advancements in the miniaturization of this hardware, as well as an effective methodology for mitigating quantum decoherence.

Another considerable, necessary development in the quantum computing research environment is the identification of a potential quantum advantage for tasks fed into a grid environment. Here, certain tasks, when allocated to quantum systems, can be computed significantly faster than digital computers. Conversely, a variety of computational tasks are better suited to be handled by classical-style machinery, as cost and qubit decoherence is a primary consideration in the large-scale realization of quantum grid computing.

## 8. Conclusion

Quantum computing for use in aerospace simulation may serve as a significantly impactful approach to the problem of high computing costs for common simulation requirements. The applicability of the inherent parallelism and ability to expedite certain matrix operations is a key element to the potential for aerospace simulation enhancements brought by quantum computing.

Further, the heterogeneous nature of a quantum computing grid environment may be effective in managing task allocation of aerospace systems connected over this network, effectively distributing computing tasks to the system best suited to the task and providing a number of other benefits, such as increased information throughput and geographical consideration of aerospace systems connected over the network. Similarly, a grid-based network may be potentially useful in providing quantum computing simulation software to an individual/organization requiring it, regardless of the geographical location of the computing hardware.

The potential for integrating principles of quantum key distribution for large-scale cyber-physical environments is also discussed. Implementing new quantum cryptographic frameworks for network security serves as a potentially impactful approach to the safety of the aerospace systems connected over this network. Alternatively, the advent of capable quantum computers presents a variety of challenges in the safety of these assets, as quantum computers are considered a key threat to currently implemented encryption methodologies.

Quantum computing simulation was also discussed as a potentially impactful tool to expedite advancements in quantum computing. A general, arbitrary scenario for the cascade of advancements resulting from capable quantum computing simulation systems as a tool for advancements in quantum computing hardware was analyzed. In this scenario, the simulation served as a tool for understanding what environmental/software changes would improve the efficacy of quantum computing hardware. Further, these possibly effective changes are then extrapolated and applied to current implementations of quantum computing systems. This may then repeat indefinitely.

## Acknowledgements

The work presented in the paper was supported, in part, by the U.S. National Science Foundation (NSF Award # 1757659).

## References

[1] Y. Cao *et al.*, “Quantum Chemistry in the Age of Quantum Computing,” *Chemical Reviews*, vol. 119, no. 19. American Chemical Society, pp. 10856–10915, Oct. 09, 2019, doi: 10.1021/acs.chemrev.8b00803.

[2] F. Bova, A. Goldfarb, and R. G. Melko, “Commercial applications of quantum computing,” *EPJ Quantum Technology*, vol. 8, no. 1. 2021, doi: 10.1140/epjqt/s40507-021-00091-1.

[3] R. Folman, “Material science for quantum computing with atom chips,” *Quantum Inf. Process.*, vol. 10, no. 6, 2011, doi: 10.1007/s11128-011-0311-5.

[4] Stephen Shankland, “Quantum computers could crack today’s encrypted messages. That’s a problem.,” *Cnet*, May 2021.

[5] W. Buchanan and A. Woodward, “Will quantum computers be the end of public key encryption?,” *J.*

*Cyber Secur. Technol.*, vol. 1, no. 1, 2017, doi: 10.1080/23742917.2016.1226650.

[6] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum machine learning," 2017, doi: 10.1038/nature23474.

[7] L. Lamata, "Quantum machine learning and quantum biomimetics: A perspective," *arXiv*. 2020, doi: 10.1088/2632-2153/ab9803.

[8] B. Muruganantham, P. Shamili, S. Ganesh Kumar, and A. Murugan, "Quantum cryptography for secured communication networks," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 1, 2020, doi: 10.11591/ijece.v10i1.pp407-414.

[9] H. Mäkelä and A. Messina, "N-qubit states as points on the Bloch sphere," *Phys. Scr.*, vol. T140, 2010.

[10] J. Roffe, "Contemporary Physics Quantum error correction: an introductory guide Quantum error correction: an introductory guide," vol. 60, no. 3, pp. 226–245, 2019, doi: 10.1080/00107514.2019.1667078.

[11] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *npj Quantum Inf.*, vol. 2, no. 1, pp. 1–9, 2016, doi: 10.1038/npjqi.2016.21.

[12] D. Lu *et al.*, "Simulation of chemical isomerization reaction dynamics on a NMR quantum simulator," *Phys. Rev. Lett.*, vol. 107, no. 2, 2011, doi: 10.1103/PhysRevLett.107.020501.

[13] A. B. de Avila, R. H. S. Reiser, M. L. Pilla, and A. C. Yamin, "State-of-the-art quantum computing simulators: Features, optimizations, and improvements for D-GM," *Neurocomputing*, vol. 393, 2020, doi: 10.1016/j.neucom.2019.01.118.

[14] M. V. Cook, "Aerodynamic Modelling," *Flight Dyn. Princ.*, pp. 353–369, 2013, doi: 10.1016/B978-0-08-098242-7.00012-2.

[15] B. M. Boghosian and W. Taylor IV, "Simulating quantum mechanics on a quantum computer," *Phys. D Nonlinear Phenom.*, vol. 120, no. 1–2, 1998, doi: 10.1016/S0167-2789(98)00042-6.

[16] A. K. Noor, "Intelligent Adaptive Cyber-Physical Ecosystem for Aerospace Engineering Education, Training, and Accelerated Workforce Development," *J. Aerosp. Eng.*, vol. 24, no. 4, 2011, doi: 10.1061/(asce)as.1943-5525.0000128.

[17] M. R. Anderson, "A simulation framework for aerospace design education," *51st AIAA Aerospace Sciences Meeting including the New Horizons Forum and Aerospace Exposition 2013*. 2013, doi: 10.2514/6.2013-659.

[18] K. V. Dyshlevoi, V. E. Kamensky, and L. B. Solovskaya, "MARSHALLING IN DISTRIBUTED SYSTEMS: TWO APPROACHES," *Citeseer*, 1997.

[19] C. Schimpf *et al.*, "Quantum cryptography with highly entangled photons from semiconductor quantum dots," *Sci. Adv.*, vol. 7, no. 16, 2021, doi: 10.1126/sciadv.abe8905.

[20] S. O. Bamgbose, X. Li, and L. Qian, "Trajectory tracking control optimization with neural network for autonomous vehicles," *Adv. Sci. Technol. Eng. Syst.*, vol. 4, no. 1, 2019, doi: 10.25046/aj040121.

[21] L. M. Duan and G. C. Guo, "Suppressing environmental noise in quantum computation through pulse control," *Phys. Lett. Sect. A Gen. At. Solid State Phys.*, vol. 261, no. 3–4, 1999, doi: 10.1016/S0375-9601(99)00592-7.

## BIOGRAPHY

***Dominic Rosch-Grace*** *is a computer science student at the North Dakota State University. He is the founder and president of the Quantum Computing Explorers organization. He has spent the past year-and-a-half researching quantum computing theory and applications. His primary research interests are quantum artificial intelligence, quantum cybersecurity, and quantum software development.*

***Jeremy Straub*** *is the Director of the NDSU Institute for Cyber Security Education and Research and an Assistant Professor in the Department of Computer Science at the North Dakota State University. He holds a Ph.D. in Scientific Computing, an M.S. and an M.B.A. and has published over 70 journal articles and over 250 full conference papers, in addition to making numerous other conference presentations. Straub's research spans the continuum between technology, commercialization and technology policy. In particular, his research has recently focused on security, privacy, robotic command and control, aerospace command and 3D printing quality assurance. Straub is a member of multiple technical societies and served as a track or session chair for numerous conferences.*