Open Access License Notice

Multidisciplinary Quantum Cybersecurity Research for the Undergraduate Laboratory

Brian Robert Callahan
Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, USA
0000-0002-1797-8633

Keenan Schilp
Dept. of Electrical, Computer & Systems Engineering
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0001-0072-0169

Quinn Colognato
Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0005-1274-4685

Emily Goldman
Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0007-3064-106X

Shoshana Sugerman
Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0002-9058-6828

Aanya Mehta
Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0002-5651-3385

Angela Imanuel
Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0008-0562-8629

Kaitlin Kaii
Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0006-2509-0665

Hannah Rose
Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, USA
0009-0008-1532-1305

Abstract—Quantum computing has a critical need to be integrated into the undergraduate classroom to meet the needs of cybersecurity education in the 21st Century and to prepare a robust quantum workforce. A cybersecurity laboratory that specializes in undergraduate research explored a pair of quantum security projects in order to develop the foundations of a rich pedagogy to realize these needs: one on cracking pseudo-RSA, and one on understanding the limitations of quantum machine learning in aiding LLM development and refinement. This paper explores why this integration is necessary, explicates the research projects undertaken by these undergraduate researchers, and discusses their contributions to applied quantum security. Our contribution is to provide a template for how to quickly and effectively establish a multidisciplinary quantum security pedagogy for undergraduate students, provide example projects that can be adapted to student interests and abilities, and demonstrate how to enroll students from a wide variety of disciplines, increasing diversity and resiliency in quantum cybersecurity and cybersecurity broadly.

Keywords—*quantum computing, cybersecurity, pedagogy, research, quantum security, diversity, resiliency*

I. INTRODUCTION

When our university purchased a quantum computer to be housed on campus, an enormous wave of excitement swept through the community. Faculty and students alike would have unfettered access to a state of the art machine, day or night, for purposes ranging from targeted research to play and experimentation. In this way, the arrival of the quantum computer heralded a return to days of old where room-filling, almost mythical, machines stood in majesty while the curious got to work exploring its ins and outs, and creating not simply solutions to problems but a new culture around the machine [1].

In celebration of the arrival, our university held a three-day symposium around quantum computing, culminating in the ribbon cutting and the machine being permanently turned on. Among the many celebrations was a poster session featuring student research projects using quantum computing and other related disciplines. The interdisciplinary nature of quantum computing brought together a variety of disciplines, including mathematics, computer science, physics, and has the potential to incorporate many additional disciplines as quantum utility, the characteristic of quantum computation to be at least one of faster, more accurate, or less energy intensive than similarly equipped classical computation [2], is achieved for an increasing number of problems.

This paper highlights two cybersecurity-focused student research projects developed for this poster session, sponsored by our university, in which students from disciplines traditionally thought of as inside the quantum

space and students from disciplines traditionally thought of as outside the quantum space worked together. These projects showcase our experiences teaching quantum cybersecurity to a wide variety of students, many of whom had no direct experience in quantum prior to participating.

This report contributes to the literature on quantum cybersecurity pedagogy. Where we have particular insights that add significant contribution to the literature is two-fold: first, in demonstrating how to harness the excitement around quantum cybersecurity to teach holistic research skills to teams of predominantly lower-level undergraduate students; and second, in our exploration of social science and humanities questions in one of the projects around the potential for quantum algorithmic bias as a viable and interesting field of inquiry for quantum cybersecurity research.

Students will speak in their own voices in this paper as to their learning experience and what they believe learning research skills in the context of a quantum security research project brought to their education that could not have otherwise been achieved. That is to say, this paper is the first-hand accounts of the students who participated in the research projects. The projects are presented in a way to be approachable by and inspiring to other students who are just beginning their quantum security and research journeys. We present these stories to encourage other educators to expand their horizons as to the types of students and projects to bring into the quantum security world.

II. BACKGROUND

As quantum computing matures, there will be an ever-increasing need for skilled professionals across many quantum-enhanced disciplines. Cybersecurity will be no different. It remains important to diversify the cybersecurity field; the industry struggles to enroll and retain women [3]. We believe that we must start now if we are to build resiliency through diversity in quantum cybersecurity. This requires the routine teaching of quantum and cybersecurity skills to students, but also thinking more broadly as to what counts as quantum cybersecurity research and who should be taking part in such research. It will be too late if we wait until quantum matures to begin asking these questions and making appropriate interventions.

In the last few years, there has been a surge in interest focused on teaching the next generation about quantum computing, some of which is designed for students as young as elementary school through the National Q-12 Education Partnership [4]. There are also reports of educational work done at the high school level to teach quantum using a hands-on approach and targeting students who may have little to no experience in quantum [5].

Other universities have reported on their applied quantum coursework designed for undergraduate students [6] and new approaches to quantum ethics education [7]. Work has also been done specifically on the teaching of quantum cybersecurity, including e-learning platforms [8] and virtual 3D educators for quantum cryptography [9].

There is evidence that STEM diversity begins to take a hit starting around eighth grade education: around this time the gender gap in STEM begins to widen dramatically and girls lose confidence and interest in STEM by high school [10]. Advancing to first-year college coursework, studies show that women are more likely to drop out of STEM majors after Calculus I, citing in part a loss of confidence in mathematical abilities [11]. That is to say, there are several steps along the way that threaten to damage the resiliency of the cybersecurity industry through lack of diversity throughout STEM education. But with appropriate interventions, we can work to counteract these threats and build a more resilient cybersecurity.

We build on this work by presenting guidance on how educators and students alike can implement many of these insights in two different quantum cybersecurity research projects: the first on cracking pseudo-RSA and the second on using quantum-enhanced Generative AI to comment on quantum ethics and quantum algorithmic bias. These projects are designed in such a way as to address the above points towards making a more resilient cybersecurity industry through making conscious efforts to widen the net of multidisciplinary research using quantum cybersecurity as the vehicle, hoping to make cybersecurity as a whole more appealing to students who might never have considered it an option.

III. PROJECT 1: CRACKING PSEUDO-RSA

The first project group, comprised of Sophomore and Junior level students in Electrical, Computer, and Systems Engineering and Information Technology, sought to use the quantum computer to crack an implementation of pseudo-RSA encryption using Shor's algorithm. This project required students to research how to use the Qiskit IDE to write quantum circuits, understand the state of the art in quantum cryptographic attacks, compromise with the current hardware limitations of quantum computers, and build software with an eye towards the future so as to create a starting point for future research that can scale with advancements in quantum hardware.

Students needed first to grapple with a range of preliminary knowledge that they had not received in their coursework: complex linear algebra, quantum state vectors, and quantum operations, finally leading to test projects reconstructing famous algorithms such as the Deutsch-Jozsa algorithm [12][13] and a solution to Simon's problem [14].

Students could then turn their attention to learning how to search literature to understand the state of the art in quantum cryptographic attacks.

Breaking pseudo-RSA with a quantum machine is possible for small key sizes, far smaller than today's common bit sizes of 2048. However, work is progressing rapidly to be able to crack RSA bit sizes in the range of 2048, one of the more

common bit sizes due to its resistance against brute force attacks by classical computers [15]. Using classical computers, the largest bit size cracked to date is 829, done in 2020 utilizing a computation time of roughly 2700 core-years [16].

Best estimates of the number of qubits required to crack encryption using such key sizes have dropped from billions [17] to ranges from approximately twenty million [18] down to 13,436 with multimode memory [19]. These drops in number of qubits also come with realistic timescales for cracking such encryption: we can imagine that it would be difficult to meaningfully claim that quantum computers can crack modern cryptographic systems if it can only do so on the order of tens of thousands or millions of years. Gouizen and Sangouard, in addition to their estimation of 13,436 qubits, also estimate it would take 177 days to crack 2048-bit RSA integers with their system [19]. Though still not immediate, this timescale is certainly within the realm of exceedingly dangerous; it is almost certainly the case that most organizations have secrets that need to be protected longer than six months. Today's most powerful quantum computers have qubits numbering just over 1,000, with aims to produce quantum computers with over 15,000 qubits by the end of the decade [20].

Armed with knowledge about the state of the art in quantum cryptographic attacks and an understanding of the latest in theoretical advancements, this group of students next devised an experiment to see how feasible cracking pseudo-RSA would be on our university's quantum computer.

The students wrote their own implementation of a pseudo-RSA cryptosystem in the C++ programming language that permitted users to input the bit size for a particular encryption session. It then allowed a message to be input. The implementation would then generate a public and private key for the requested bit size, encrypt the message with the public key, and display the encrypted message.

The students then needed to code an implementation of Shor's algorithm [21] that could be executed on the quantum computer. Shor's algorithm is well-known for being a key component in using quantum computing to crack RSA encryption. Developed in the mid-1990s, long before quantum computers were realized, teams are now able to implement the algorithm. Shor's algorithm does not do all of the work of cracking RSA; it does the work of period finding and its output is combined with classical algorithms to complete the cracking [22].

Unlike classical computers, which can be programmed with any number of high-level languages that somewhat resemble human languages, no such high-level or truly any programming languages yet exist for quantum computers. The students needed to use their newly gained knowledge built off the successes of implementing the Deutsch-Jozsa algorithm and their solution to Simon's problem to write even more complex *circuits* using *gates*, nearly analogous to laying out the organization of the individual transistors in classical computers. As of now, quantum programming is mature enough that certain groups of circuits are offered as a singular unit of organization, for example the Quantum Fourier Transfer (QFT), but nevertheless these groups of circuits are being arranged by hand by quantum programmers to create a larger circuit to be executed.

Figure 1 is the quantum circuit implementing Shor's algorithm that the students created and executed on the quantum computer. Note the "program" is the physical organization of these gates built up to create a larger circuit, which is what is executed on the quantum computer.

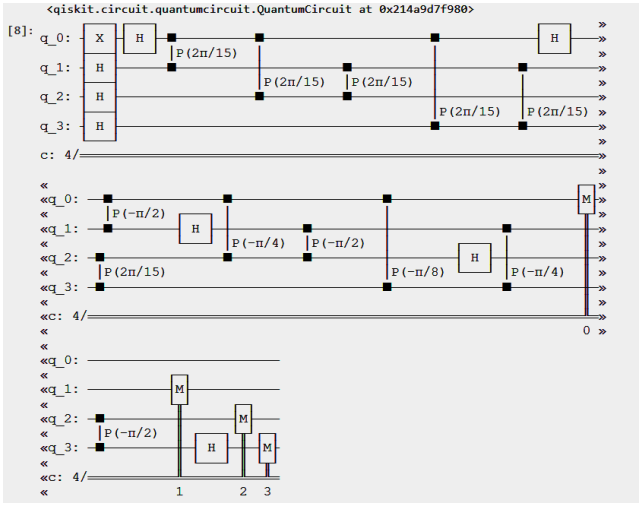

Fig. 1. Quantum circuit implementing Shor's algorithm

These students were ultimately able to reliably crack encryption for 6-bit key sizes. While this is far from the 2048 bits that we routinely see in RSA systems today, or even the 829 bits that is the best classical machines can do, the combination of theoretical work the students engaged with and the practical work performed in their experiment demonstrates that it is the reality today that pseudo-RSA can be cracked using quantum systems on real hardware, at a level that undergraduate students can learn and understand within the scope of a single semester.

As quantum systems grow in number of qubits, and thusly power, the students intend to continue to optimize and improve their circuit to march in lockstep with future hardware advances. That is to say, as quantum computer hardware improves, the students will be able to further push the bit size for keys that can be reliably cracked.

The last task these students were able to accomplish was the inclusion of quantum error mitigation. The students initially did their work on a perfect, error-free, quantum simulator. Real quantum systems are susceptible to *noise*, effectively the production of errors due to imperfect interactions [23]. This noise can be caused by any number of factors; one such factor is natural vibrations in the environment. When our university installed its quantum

computer, the floor upon which the machine is housed needed to be reengineered so as to minimize such environmental vibrations as much as possible, thereby reducing noise and therefore errors in the quantum processing, as much as possible.

Even with the most well-engineered infrastructure, techniques such as error mitigation [23] and error correction [24] are critically important. The students were able to implement error mitigation as a stretch goal in their research, so that transient noise could be detected and computation redone in the event of unacceptable noise. As with improvements in bit size, the error mitigation will be carried forward in future iterations of their circuit to take advantage of improvements in quantum hardware; as a result, we should expect that cracking pseudo-RSA and eventually real RSA will not only be more possible but more reliable as more powerful quantum hardware is designed and implemented, and eventually arrives on campus through any future upgrades our quantum computer may receive.

IV. PROJECT 2: QUANTUM MACHINE LEARNING AND QUESTIONS OF QUANTUM ALGORITHMIC BIAS

Multidisciplinary research within quantum cybersecurity must not be gatekept away from social science and humanities students, and other students whose disciplines might not be traditionally considered within the realm of quantum computing or cybersecurity. Indeed, these students have much to offer as their questions to probe the overall mission of creating safe and secure quantum computing may go unasked by students in disciplines considered traditional to quantum computing and cybersecurity. Disciplines such as Science and Technology Studies (STS) have offered insight into how computers have changed society and vice-versa [25][26] and provided insights into how to improve diversity in the field [27]. It is our belief that incorporating students in STS with our Information Technology and Computer Science students would yield better questions and better analysis of the research. This project demonstrates that it is not too early to widen what counts as quantum cybersecurity research and is not too early to welcome insights from more disciplines.

The primary focus of this research was one that the students themselves brought to the table, around the question of quantum algorithmic bias: that is to say, quantum algorithms, much like traditional computing algorithms, may in fact bring about unfair discrimination against specific groups of people as a result of human influence on the design and implementation of algorithms and code [28]. Algorithmic bias is well studied in the literature [29] but primarily focused on classical algorithms.

As the students in this project were all Freshmen and Sophomores, many of them had recently completed, or were currently taking, a required freshman-level humanities course that explored questions around the co-production of culture, society, and technology. As such, algorithmic bias was a topic that they were actively grappling with, and the students rightly pointed out that there is no reason to assume that quantum algorithms would be any different in this respect than classical algorithms. After all, these algorithms were designed and implemented by humans. And they did not believe it was too early to explore that question; indeed, better to explore now and come up with little than wait until it is too late and find there is much to undo.

As privacy is an interlocking concern with cybersecurity in a wide array of applications such as smart cities [30][31][32], autonomous vehicles [33], artificial intelligence [34] including Generative AI [35][36][37][38], and more, these students wanted to effectively "get ahead" of concerns they believed would emerge around the potential for quantum algorithms to exhibit a similar potential for discrimination as their classical counterparts, and therefore help to push forward the conversation around quantum security and privacy early.

The students learned that, while much has been offered on the relationship between privacy and cybersecurity with traditional algorithms, there was significantly less when attention was turned to quantum algorithms. Students focused their attention on literature situating first developments of a roadmap for the development of quantum computing ethics [39] and quantum fair machine learning [40] to guide their efforts. This group wanted to begin the process of developing best practices for quantum Generative AI, which has already been proposed for classical Generative AI [41].

The students were considering research questions well-known in the literature for classical machine learning such as perpetuating gender stereotypes [42]. What the group hoped to accomplish was to see that, depending on how they coded their quantum machine learning algorithms, and depending on what input data they used, to see a visible difference in output. Perhaps one that would make it noticeable that there may be gender disparities in their textual output.

As a group, the students developed a project that could serve as a preliminary basis to discuss the potential for quantum algorithmic bias: the development of a simple large language model (LLM) that could be implemented on both a classical computer and a quantum computer. Students began by installing and learning how to use NanoGPT [43], a small Python-based implementation of an LLM, and training it on Project Gutenberg text, chosen so as to avoid any potential questions of copyright issues which currently plague larger LLM implementations [44].

After the students were successful in creating their own Project Gutenberg-trained LLM with NanoGPT on classical computers, they tried to replicate the effort through quantum circuits. The effort did not translate to quantum computers; hardware limitations prevent more than a single small piece of an LLM to be built. This group then needed to reorganize and ask themselves if they could still learn and share something meaningful about the intersection of quantum computing and algorithmic bias without implementing a full LLM.

The group settled on a part of speech analyzer. While this was far less than a full LLM, it could in theory be plugged into NanoGPT or another LLM implementation and still offer discernable differences and could still be compared to a comparable classical system. The group discovered that classical fine tuning and quantum fine tuning looked very similar in terms of coding; the primary difference is using a Variational Quantum Classifier (VQC) to do the fine tuning.

While the part of speech analyzer was ultimately a standalone project, the group was able to see that differences in training text input and implementation of the quantum circuit impacted the accuracy and output of the part of speech analyzer. To extrapolate, the group believes there is no reason to assume that quantum algorithms *won't* be susceptible to the same algorithmic bias issues as classical algorithms, and we should start to tend to those issues now. While the excitement of quantum is real and much technical work still needs to be done, it is not too early to tend to the human effects of quantum computing.

V. CONCLUSION

We look back on our projects with feelings of success and anticipation for the future. Quantum cybersecurity can be successfully brought into the undergraduate research laboratory across a wide range of interests, concerns, and disciplines. We encourage educators to use the examples we discussed in this paper to bring these projects and related projects to their undergraduate students. A cybersecurity research laboratory was able to teach eight undergraduate students the fundamentals of research through exciting quantum cybersecurity projects, devised and run by the students themselves. We encourage this effort to be replicated at other institutions.

Reflecting on the experience, the students discussed their trailblazing into new territory that meant having to routinely push themselves out of their comfort zones. They discussed their lack of understanding of the complex structure of how research integrates with the university and broader world prior to engaging in these projects. The culminating poster session brought our university together and invited the broader world to come to us to explore the exciting world of quantum cybersecurity. Students reflected on the applied nature of their work: needing to rely on their own insights to create, shape, and plan new projects.

All but one of the researchers across both groups were women. We know that the cybersecurity industry struggles to enroll and retain women [3]; it is our hope that our approach to quantum security research, an approach that purposefully seeks to include students from disciplines such as STS and other disciplines not traditionally considered inside quantum computing, can both serve to engage insights now considered crucial in the ethics and resilience of classical computing and build that resilience through inclusion and diversity—diversity in the individuals themselves and their experiences, expertise, and ideas. Cybersecurity needs thinkers from a wide variety of disciplines; we can leverage the excitement of quantum computing to bring those students into the cybersecurity fold with research well-crafted at the intersections of quantum and cybersecurity, and engaging with their concerns as a vehicle to build interest in the field, and ultimately create a more resilient cybersecurity.

Indeed, resilience was mentioned several times by students across both projects. Because quantum computing, and by extension quantum cybersecurity, is so new, students felt like they sometimes lacked enough reference material for guidance. However, they mentioned the novelty and uniqueness of their work kept them focused on the challenges and gave them a shared mission to work together in their group to overcome potential hurdles. It is our hope that the resilience instilled in these students over the course of their projects leads them to be champions in the cybersecurity field for women and other underserved groups.

As quantum cybersecurity matures, the need for meaningful and exciting projects to teach research and quantum skills will become ever more important. We believe the research projects introduced in this paper are viable single-semester projects for predominantly lower-level undergraduate students across a wide range of disciplines. We encourage others to use our examples and contribute further examples of their own in order for the larger cybersecurity educational community to quickly and effectively establish a multidisciplinary quantum security pedagogy for undergraduate students in the context of the research laboratory.

ACKNOWLEDGEMENT

We would like to acknowledge our university's Office of Undergraduate Education, who graciously sponsored these projects.

No Generative AI was used in the research or writing of this paper.

REFERENCES

[1] S. Levy, *Hackers: Heroes of the computer revolution*. Garden City, N.Y.: Anchor Press/Doubleday, 1984. doi: https://dl.acm.org/doi/10.5555/1859398.

[2] N. Herrmann et al., "Quantum utility – definition and assessment of a practical quantum advantage," *2023 IEEE International Conference on Quantum Software (QSW)*, Chicago, IL, USA, 2023, pp. 162-174, doi: 10.1109/QSW59989.2023.00028.

[3] "2023 ISC2 Cybersecurity workforce study: How the economy, skills gap and artificial intelligence are challenging the global cybersecurity workforce." Accessed: May 20, 2024. [Online]. Available: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf

[4] "National Q-12 Education Partnership | Supporting a diverse, quantum-ready workforce.," *q12education.org*. https://q12education.org/

[5] P. P. Angara, U. Stege, A. MacLean, H. A. Müller and T. Markham, "Teaching Quantum Computing to High-School-Aged Youth: A Hands-On Approach," in *IEEE Transactions on Quantum Engineering*, vol. 3, pp. 1-15, 2022, Art no. 3100115, doi: 10.1109/TQE.2021.3127503.

[6] F. Galetto, H. H. López, M. Rahmati, J. Sang, and C. Yu, "Experience in teaching quantum computing with hands-on programming labs," *The Journal of supercomputing*, Mar. 2024, doi: https://doi.org/10.1007/s11227-024-06001-3.

[7] J. É. Arrow, S. E. Marsh and J. C. Meyer, "A Holistic Approach to Quantum Ethics Education," *2023 IEEE International Conference on Quantum Computing and Engineering (QCE)*, Bellevue, WA, USA, 2023, pp. 119-128, doi: 10.1109/QCE57702.2023.20332.

[8] R. Mallipeddi, C. Schaaf, M. Subramaniam, A. Parakh and S. Weitl-Harms, "A Framework for an Intelligent Adaptive Education Platform for Quantum Cybersecurity," *2023 IEEE Frontiers in Education Conference (FIE)*, College Station, TX, USA, 2023, pp. 1-5, doi: 10.1109/FIE58773.2023.10343010.

[9] S. McDermott, S. Vadla, V. Bommanapally, A. Parakh, M. Subramaniam, and E. Ostler, "Teaching Quantum Cryptography Using a Virtual 3D Educator: QuaSim," *LOUIS*, 2017. https://louis.uah.edu/cyber-summit/ncs2017/ncs2017papers/10/.

[10] L. M. MacLean, *Cracking the code: How to get women and minorities into STEM disciplines and why we must*. New York: Momentum Press, 2017.

[11] J. Ellis, B. K. Fosdick, and C. Rasmussen, "Women 1.5 Times More Likely to Leave STEM Pipeline after Calculus Compared to Men: Lack of Mathematical Confidence a Potential Culprit," *PLOS ONE*, vol. 11, no. 7, p. e0157447, Jul. 2016, doi: https://doi.org/10.1371/journal.pone.0157447.

[12] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, vol. 439, no. 1907, pp. 553–558, Dec. 1992, doi: https://doi.org/10.1098/rspa.1992.0167.

[13] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, "Quantum algorithms revisited," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 454, no. 1969, pp. 339–354, Jan. 1998, doi: https://doi.org/10.1098/rspa.1998.0164.

[14] D. R. Simon, "On the Power of Quantum Computation," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1474–1483, Oct. 1997, doi: https://doi.org/10.1137/s0097539796298637.

[15] A. A. Hasib and A. A. M. M. Haque, "A comparative study of the performance and security issues of AES and RSA cryptography," *2008 Third International Conference on Convergence and Hybrid Information Technology*, Busan, Korea (South), 2008, pp. 505-510, doi: 10.1109/ICCIT.2008.179.

[16] P. Zimmerman. "[Cado-nfs-discuss] Factorization of RSA-250." *Archive.org*. Accessed: Sep. 1, 2024. [Online]. Available: https://web.archive.org/web/20200228234716/https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2020-February/001166.html

[17] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, "Surface codes: Towards practical large-scale quantum computation," *Physical Review A*, vol. 86, no. 3, p. 032324, Sep. 2012, doi: https://doi.org/10.1103/PhysRevA.86.032324.

[18] C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, p. 433, Apr. 2021, doi: https://doi.org/10.22331/q-2021-04-15-433.

[19] É. Gouzien and N. Sangouard, "Factoring 2048-bit RSA integers in 177 days with 13,436 qubits and a multimode memory," *Physical Review Letters*, vol. 127, no. 14, Sep. 2021, doi: https://doi.org/10.1103/physrevlett.127.140503.

[20] A. Pasternak. "IBM built the biggest, coolest quantum computer. Now comes the hard part." *FastCompany.com*. Accessed: Sep. 1, 2024. [Online]. Available: https://www.fastcompany.com/90992708/ibm-quantum-system-two

[21] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, 1994, pp. 124-134, doi: 10.1109/SFCS.1994.365700.

[22] H. Y. Wong, "Shor's Algorithm," in *Introduction to Quantum Computing: From a Layperson to a Programmer in 30 Steps*, 2nd ed., pp. 289-298, Cham: Springer. doi: https://doi.org/10.1007/978-3-031-36985-8.

[23] Z. Cai, R. Babbush, S. C. Benjamin, S. Endo, W. J. Huggins, Y. Li, J. R. McClean, and T. E. O'Brien, "Quantum Error Mitigation," *Reviews of Modern Physics*, vol. 95, no. 4, p. 045005, Dec. 2023, doi: https://doi.org/10.1103/RevModPhys.95.045005.

[24] S. Bravyi, A. W. Cross, J. M. Gambetta, D. Maslov, P. Rall, and T. J. Yoder, "High-threshold and low-overhead fault-tolerant quantum memory," *Nature*, vol. 627, no. 8005, pp. 778–782, Mar. 2024, doi: https://doi.org/10.1038/s41586-024-07107-7.

[25] G. L. Downey, *The machine in me: An anthropologist sits among computer engineers*. New York: Routledge, 1998. doi: https://doi.org/10.4324/9781315022611.

[26] D. E. Forsythe, *Studying those who study us: An anthropologist in the world of artificial intelligence*. Stanford University Press, 2002. doi: https://doi.org/10.1515/9781503619371.

[27] J. Davis, M. Lachney, Z. Zatz, W. Babbitt, and R. Eglash, "A Cultural Computing Curriculum," *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*, Feb. 2019, doi: https://doi.org/10.1145/3287324.3287439.

[28] B. Friedman and H. Nissenbaum, "Bias in computer systems," *ACM Transactions on Information Systems*, vol. 14, no. 3, pp. 330–347, Jul. 1996, doi: https://doi.org/10.1145/230538.230561.

[29] N. Kordzadeh and M. Ghasemaghaei, "Algorithmic bias: review, synthesis, and Future Research Directions," *European Journal of Information Systems*, vol. 31, no. 3, pp. 1–22, Jun. 2021. doi: https://doi.org/10.1080/0960085X.2021.1927212.

[30] R. Khatoun and S. Zeadally, "Cybersecurity and Privacy Solutions in Smart Cities," in *IEEE Communications Magazine*, vol. 55, no. 3, pp. 51-59, March 2017, doi: 10.1109/MCOM.2017.1600297CM.

[31] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," *Sustainable Cities and Society*, vol. 50, no. 101660, p. 101660, Oct. 2019, doi: https://doi.org/10.1016/j.scs.2019.101660.

[32] E. Vattapparamban, İ. Güvenç, A. İ. Yurekli, K. Akkaya and S. Uluağaç, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, Paphos, Cyprus, 2016, pp. 216-221, doi: 10.1109/IWCMC.2016.7577060.

[33] A. Taeihagh and H. S. M. Lim, "Governing Autonomous vehicles: Emerging Responses for safety, liability, privacy, cybersecurity, and Industry Risks," *Transport Reviews*, vol. 39, no. 1, pp. 103–128, Jul. 2019, doi: https://doi.org/10.1080/01441647.2018.1494640.

[34] C. Tschider, "Regulating the IoT: Discrimination privacy and cybersecurity in the artificial intelligence age", *Denver Law Rev*., vol. 96, no. 1, pp. 87-143, 2018. doi: https://dx.doi.org/10.2139/ssrn.3129557.

[35] M. Gupta, C. Akiri, K. Aryal, E. Parker and L. Praharaj, "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy," in *IEEE Access*, vol. 11, pp. 80218-80245, 2023, doi: 10.1109/ACCESS.2023.3300381.

[36] K. Michael, R. Abbas and G. Roussos, "AI in Cybersecurity: The Paradox," in *IEEE Transactions on Technology and Society*, vol. 4, no. 2, pp. 104-109, June 2023, doi: 10.1109/TTS.2023.3280109.

[37] Y. Chen and P. Esmaeilzadeh, "Generative AI in Medical Practice: In-Depth Exploration of Privacy and Security Challenges," *Journal of Medical Internet Research*, vol. 26:e53008, Mar. 2024, doi: https://doi.org/10.2196/53008.

[38] C. Novelli, F. Casolari, P. Hacker, G. Spedicato, and L. Floridi, "Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity," *arXiv.org*, Feb. 19, 2024. https://arxiv.org/abs/2401.07348. doi: https://doi.org/10.48550/arXiv.2401.07348.

[39] E. Perrier, "Ethical Quantum Computing: A Roadmap," *arXiv:2102.00759 [quant-ph]*, Apr. 2022, Available: https://arxiv.org/abs/2102.00759. doi: https://doi.org/10.48550/arXiv.2102.00759.

[40] E. Perrier, "Quantum Fair Machine Learning," *AIES '21: Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society*, pp. 843-853, USA, May 2021, doi: https://doi.org/10.1145/3461702.3462611.

[41] D. Roselli, J. Matthews, and N. Talagala, "Managing Bias in AI," *Companion Proceedings of The 2019 World Wide Web Conference*, pp. 539–544, May 2019, doi: https://doi.org/10.1145/3308560.3317590.

[42] [42] H. Cramer, J. Garcia-Gathright, A. Springer, and S. Reddy, "Assessing and addressing algorithmic bias in practice." Interactions, vol. 25, no. 6, pp.58-63, 2018, doi: https://dx.doi.org/10.1145/3278156.

[43] A. Karpathy. *NanoGPT*. GitHub. Accessed: Jan. 29, 2024. [Online]. Available: https://github.com/karpathy/nanoGPT

[44] P. Samuelson, "Generative AI meets copyright," *Science*, vol. 381, no. 6654, pp. 158–161, Jul. 2023, doi: https://doi.org/10.1126/science.adi0656