ACADEMIA Tech Frontiers Journal

Quantum Computing and Its Implications for Cybersecurity

Muhammad Javed [a]

[a] Department of Computer and Information Sciences, Pakistan Institute of Engineering and Applied Sciences (PIEAS), Islamabad, Pakistan(javed123@gmail.com)

Article Info:
Received: May 07, 2025
Revised: May 21, 2025
Accepted: June 11, 2025

Corresponding Author:
Muhammad Javed
(javed123@gmail.com)

ABSTRACT

The subsequent sport changer in computational strength is quantum computing, which additionally has the ability of presenting answers to tough issues that the classical structures aren't capable of handle. Although this technological step forward holds guarantees of creating a few technological achievements in fields like drug discovery, optimization, and synthetic intelligence, it makes it very bodily tough to cyber security. Conventional cryptographic hardware like the ones counting on each RSA and ECC algorithms is liable to quantum assaults ensuing in algorithms like the ones invented with the aid of using Shor. In this paper, the writer narrows right all the way down to the duality of quantum computing or its capability to convert the manner issues are labored out or the manner it's far destabilising modern virtual protection structures. Focus is at the feel of urgency to create encryptions that the quantum can smash and the global scramble in quantum-associated studies, in addition to the moral and political components of the issue. With a vital evaluation of possibilities and threats of quantum computing, the observe has proven a dire want to put together proactive strategies to make certain the integrity of facts withinside the corporation at some point of the post-quantum.

Keywords

Quantum computing, cybersecurity, cryptography, post-quantum algorithm, Shor algorithm, virtual security, quantum resistance

INTRODUCTION

One of the predominant technological revolutions of the 21 st century is the fast improvement of quantum computing. In evaluation to the classical computer systems which manage records in binary (0s and 1s), quantum computer systems are managed through qubits, which might be able to being in superposition, for that reason letting them calculate on a scale by no means pondered before. The cappotential permits quantum structures to clear up issues that have been formerly taken into consideration computationally infeasible inside possible time scales with various programs withinside the clinical studies discipline in addition to monetary modeling. But there's with it an existential undertaking to virtual safety.

Modern cybersecurity is primarily based totally on cryptographic algorithms just like the RSA, Diffie-Hellman, and elliptic-curve cryptography. These structures use touchy facts with the demanding situations of mathematical troubles of integer factorization and discrete logarithms. This stability is threatened to be dissatisfied via way of means of quantum computing. In 1994 Shor recommended an set of rules that during principle a quantum pc effective sufficient ought to compromise not unusualplace encryption structures on a police time basis, leaving maximum of the virtual infrastructure withinside the current at risk. Since interactive international communication, trade, and governance have turn out to be an increasing number of reliant on virtual faith, the demanding opportunities of quantum era pose urgent demanding situations of preparedness.

Governments and companies international are closely enticing withinside the quantum race, with an appreciation that they're now no longer simplest introducing the opportunities of innovation however countrywide safety is likewise at risk. U.S., China and the European Union are main studies efforts, and companies along with NIST (National Institute of Standards and Technology) are at the frontline to provide you with quantum resistant cryptographic standards. Nevertheless, questions about how quantum supremacy of cryptanalysis will show up nonetheless linger, generating a slim hole wherein virtual structures can nonetheless be vulnerable.

In addition, the outcomes of quantum computing aren't restrained to technical factors. The scenario is in addition complex with the aid of using the moral issues surrounding equitable access, the coverage arguments approximately law and the opportunity of energy imbalances at the geopolitical level. When quantum abilties are managed via way of means of a small range of actors, the worldwide gadget of cybersecurity would possibly turn out to be extra risky than ever. Therefore, the dialogue of quantum computing isn't always confined to the improvement of era however is intently interconnected with the topics of trust, governance, and equity.

This paper is positioned on the nexus among era and safety and is a important look at the effect of quantum computing at the paradigm of cybersecurity. This examine will assist the modern instructional and policymaking dialogue on the way to put together to be withinside the post-quantum international via way of means of inspecting the dual elements of quantum progress: its capacity to decorate computational electricity and its cappotential chance to the protection of the virtual international.

Objectives

1. To decide the threats that quantum computing can carry to the present day cryptographic and cybersecurity models.
2. To determine what new tactics are underway, in particular quantum-resistant encryption, a good way to shield the virtual infrastructure withinside the post-quantum space.

Research Questions

1. What has quantum computing completed to disillusioned the standards of the present cybersecurity or encryption infrastructures?
2. Which varieties of technological, coverage, and moral answers are important to deal with the risks associated with quantum-primarily based totally cyber attack?

LITERATURE REVIEW

Quantum computing has end up a groundbreaking discipline, a place this is counseled to alternate how the computing enterprise can evolve via way of means of pushing the boundary past the geographical regions of classical computing, which on the equal time additionally creates good sized demanding situations to cybersecurity. The included literature indicates the equal homes that render quantum computing a which means strength are the primary limitations to the portability of cryptography on one base of virtual communications. The classical encryption algorithms, RSA and elliptic-curve cryptography, are primarily based totally at the infeasibility of factorizing big high numbers, or discrete logarithmic computations, making use of classical stateful computation. It has continually been proper that when the concept of scalable quantum computer systems comes actual, there are algorithms like that of Shor, as a way to be taken into consideration a unnecessary shape of quantum pc as they could factorize exponentially quicker than some thing classical (Shor, 1994; Mosca, 2018). Researchers have consequently described quantum computing now no longer as a technological innovation possibility however additionally as a virtual protection disaster to return back withinside the world.

This trouble is critical as numerous research examine timelines of what's projected to take place in exercise in quantum assaults. Although the optical quantum computer systems are actually constrained on the steadiness of quantum bits and dimension blunders, widespread efforts with the aid of using governments and era agencies have accelerated the improvement of fault-tolerant qubit computer systems (Arute et al., 2019). Such boom has caused the worry of so-called, so-called, harvest now, decrypt later, assaults wherein the encrypted statistics transmitted these days can be sidelined to be accessed and decrypted on the cease of time as quantum energy will become a reality (Chen et al., 2016). This vulnerability extends to the regions of giant regard, like kingdom communications, scientific statistics, and business, wherein the data nice wishes do not need to be saved at some point of many years however all through years.

When discussing the worldwide coverage reaction, the literature additionally singles out the reaction of the National Institute of Standards and Technology (NIST) with initiatives like its Post-Quantum Cryptography Standardization challenge this is presently trying out the algorithms susceptible to quantum assaults (NIST, 2022). Researchers have harassed that the transfer to depend upon quantum-resistant kind is a multi-faceted procedure that can't be achieved completely thru technological innovation and desires to contain cooperation on an industrial, governmental, global level (Barker et al., 2020). Other authors declare that the unwillingness to do some thing would possibly motive a sort of a cryptographic cliff situation, wherein structures which are steady these days will fall sufferer to an apocalyptic failure almost in a single day as soon as the strength of quantum is going mainstream (Mosca & Piani, 2019).

There is likewise a parallel older frame of literature searching at whether or not quantum computing may be used to enhance cybersecurity as itself. Quantum key distribution (QKD) is primarily based totally at the mechanic regulation of quantum mechanics as it offers the capability of being incapable of encryption thru presenting the availability of steady conversation that informs any attempt to have eavesdropping (Bennett and Brassard, 1984). Other experiments in China and Europe have additionally tested viability of QKD with satellite tv for pc networks indicating a pathway to infrastructures which are quantum stable towards intrusion (Yin et al., 2017). Nonetheless, the critics recommend loss of universality of QKD implementation, wherein specialised hardware could be necessary, and it might be confined in phrases of scalability and integration with the modern structures (Scarani et al., 2009). As stated in the course of the dialogue withinside the literature, quantum technology pose a chance to the present cryptography standards, however additionally have the ability to provide new sources to bolster cybersecurity in case they're thoughtfully implemented.

A exclusive department of getting to know poses the query of quantum development alongside the moral and the geopolitical lines. Some of those authors suggest feasible unequal get right of entry to to quantum technology, wherein the technologically superior states or businesses would possibly expand unfair dominance over facts safety and set up new records inequality (Allison, 2020). The enjoy of quantum accumulation of sources in particular nations along with the United States, China, and members of the European Union brings into worry that much less effective nations are going to be installed a extra prone position, widening the worldwide cyber resilience disparity (Zeng, 2021). This is augmented with moral overdrafts of records possession and facts averting, because the ability to intercept encrypted messages may dissatisfied religion withinside the on line management conferences. Researchers consequently cause that after making debates approximately the capability of the quantum computing, a much broader scope need to be viewed, which ought to pass past technical limitations, to at least one in which equity and fairness are taken into account, in addition to global cooperation.

Another settlement obvious withinside the literature is that the shift to post-quantum protection can not be transitioned. Nevertheless, it's also divided in phrases of the exceptional techniques to be employed. Other researchers advocate a transition to hybrid fashions that deliver collectively classical and quantum-resistant cryptography withinside the transition, compromising dangers however now no longer depending but on untested answers (Alagic et al., 2020). It is others who warn that this sluggish implementation can motive imbalances withinside the network, which also can monitor susceptible factors that's the vulnerability to enemies. Empirical studies of company and governmental readiness ads a view that maximum institutes are unprepared to address quantum disruption, and aren't conscious and feature extraordinarily slow migration techniques (Bindel et al., 2020). Such a distinction among theoretical paintings and readiness dictates the preference of urgency in educating, investing, and coverage incentive to inspire the size adoption of post-quantum structures.

Industry function is likewise highlighted withinside the current studies and technological giants like IBM, Google, Microsoft and different researchers are actively looking to become aware of quantum computing studies on the subject of cybersecurity uses. Academia-enterprise-authorities collaboration is now taken into consideration the important thing to making certain that post-quantum answers are possible now no longer handiest in phrases of technological enchantment however additionally cost-effectiveness (Brod et al., 2021). There is a few push-lower back over quantum talents on the identical time, the literature warns of the risks of overhyping quantum talents. Other researchers emphasize that regardless of the fast improvement, there are nonetheless fundamental technical demanding situations, together with destruction of blunders and coherence of qubits, and so subjects will see the improvement sped up (Preskill, 2018). Saintrikes among urgency or realism are as a result a topic in circulation, due to the fact complacency and alarmism can function threats to powerful rules responding.

Put collectively, the literature offers us a complex photograph concerning the consequences of quantum computing on cybersecurity. It is each a modern danger to existent cryptographic infrastructures as an existential presence and a motive force of emergent protection invention, and a supply of each moral and geopolitical issue. The educational evaluation confirms that quantum disruption is inevitable and proactive model is necessary, even though lots can be mentioned on the rate of technological maturity, the foremost procedures of the migration, and the worldwide projects of governance which can be crucial to guarantee truthful safety. This literature indicates that making plans withinside the post-quantum generation isn't best a mission of technical issue however additionally a multidisciplinary mission to be inter-disciplinary, inter-sectoral, and inter-border.

METHODOLGY

This paper is a qualitative narrative overview design, which tries to arrange and seriously choose the more and more more growing literature on quantum computing and its impact on cybersecurity. The narrative evaluate is an mainly relevant method to this subject matter for the reason that realm of quantum technology is converting very quickly, and the literature includes lots of fields together with laptop technological know-how, cryptography, records security, ethics, and coverage. Instead of creating a meta-evaluation that has most effective quantitative evidence, the narrative method permits one-of-a-kind factors to be delivered to the fore and the thoroughness of technological, social, and geopolitical factors to be encompassed.

The reassets used to achieve statistics to be explored as part of this studies had been styles of secondary reassets, especially scholarly journals, convention papers, books, and institutional reviews posted for the duration of the time frame of 2010-2024. Peer-reviewed courses and guides of reputable corporations like National Institute of Standards and Technology (NIST), European Telecommunications Standards Institute (ETSI), and individual, principal era companies operating on quantum studies had been given precedence to be taken into consideration as credible and relevant. Digital databases, together with IEEE Xplore, technology direct, springerlink and Google scholarly have been searched with key phrases inclusive of quantum computing, cybersecurity, post-quantum cryptography, quantum key distribution, and cryptographic vulnerability. Citation chaining tripped up extra sources that received paintings that had the maximum have an impact on withinside the literature.

The criterion used to choose the reassets centered at the intersection of quantum computing and cybersecurity, be it thru a technical, pragmatic, or every other lens. Articles that have been now no longer targeted on quantum telecommunications and cybersecurity had been ignored, and people that speculated approximately the issue with out empirical and theoretical aid in addition to people who have been out of date and did now no longer constitute sizeable breakthroughs withinside the field. As many as 60 reassets had been assessed thoroughly, a pruned populace of 25- 30 then covered withinside the very last dialogue for you to preserve breadth and intensity.

The procedure of statistics evaluation became primarily based totally at the packages of thematic synthesis thru the framework provided via way of means of Braun and Clarke, (2006). Sources have been examine normally with principal arguments and unearths coded to routine issues withinside the region of the weak spot of the classical encryption, post-quantum cryptographic answers and strategy, the capability and restraints of the quantum key distribution, the demanding situations to appropriate international governance, and moral issues. These subject matters had been then in comparison and contrasted the use of them and blended right into a important verbal exchange that establishes factors of agreement, confrontation in addition to open questions. This turned into performed in order that this studies should not depend on the descriptive precis however ought to development to the analytical interpretation of the function of revitalizing quantum computing on cybersecurity.

In order to enhance validity, triangulation turned into used by factoring withinside the perspectives of academic, commercial and coverage-orientated texts which minimized the danger of bias introduced approximately through the notion of the usage of a unmarried class of reassets. Research transparency become ensured via the documentation of the quest method, inclusion criteria, and the thematic coding that permits the approach to be reproducible or criticized through the researchers withinside the destiny. Still, the studies paper acknowledges the weaknesses of a story evaluation. First, the secondary facts means that the effects are motivated through accessibility to the to be had and quantity of the studies that won't exhaust the modern-day technical advances that came about in private laboratories. Second, quantum innovation is transferring at a quick rate, and so selections can grow to be out of date withinside the current and therefore they ought to be up to date with a view to be stated on a non-stop basis. Lastly, using greater superior generation offers to pay attention the scholarship and experimentation in numerous technologically advanced international locations creates a probable geographic bias among them for the reason that perspectives of the growing global continue to be underrepresented withinside the literature.

Regardless of those shortcomings, the chosen method affords an in-intensity and vital perception into the kingdom of knowledge. It gives a good footing at the more than one components of quantum computing with a excellent wide variety of implications on cybersecurity through thoughtfully mixing the technical, moral, and coverage viewpoints and giving tips at the manner destiny studies have to be conducted.

DATA ANALYSIS AND DISCUSSION

The statistics acquired through the evaluation of academic, industry, and coverage-making reassets demonstrates that the scenario is alternatively complex as quantum computing appears to be an remarkable possibility and an existential undertaking of cybersecurity. As the evaluation demonstrates, severa factors of technical breakthroughs, institutional preparedness, and governance debates are converged pointing to the methods societies can go through the transformative effects of quantum technology. It is that this segment that summarizes what has been reviewed and discusses the effect the emergence of quantum computing has on current encryption structures the plans which might be underway to counter this hazard in addition to the dual-use abilties of the brand new quantum technology, the ethical and geopolitical implications of unequal get admission to, and the preparedness of the arena to emerge as a part of the post-quantum world.

The protection of classical cryptography to quantum assaults is one of the foremost subjects that on every occasion is found in the ones literature. The authentic conceptualization of conventional PK infrastructures (mainly fashions the usage of RSA and enforcing discrete logarithms primarily based totally on an elliptic curve) are primarily based totally at the infeasibility of: Factoring of massive integers or discrete logarithms. After all of the troubles can theoretically be solved the usage of quantum algorithms, just like the Shor algorithm, in the course of a positive quantity of time that could be a mere instance that everlasts furnished that there are extra superior quantum algorithms able to precisely fixing those troubles inside hours or maybe days; matters that classical supercomputers might require millennia earlier than completing their recurring duties are conceivable in only some hours on sufficiently superior quantum computer systems. Although its renewed implementation such assaults have now no longer been completely scaled to feasible quantum pc competencies as of but, a phenomenon known as harvest now, decrypt later is stated withinside the literature. Enemies at the moment are capable of store coded messages and wait until a realistic quantum machine is evolved while backdoors may be used to listen in on labeled records. This is a chance as a way to be extensive and the purpose why a shift went to post-quantum cryptography requirements is urgent, earlier than quantum computer systems have completely matured.

The facts spotlight the global shift in the direction of the introduction of quantum-resistant cryptography as a counter-shielding degree as well. In 2016, the Post-Quantum Cryptography (PQC) standardization task prepared through the National Institute of Standard and Technology turned into time and again given as the biggest coordinated contribution to the quantum hazard preparation. Lattice elliptic organization cryptography Candidate algorithms like CRYSTALS-Kyber and Dilithium were decided on as finalists to turn out to be the situation of standardization, with deployment because of begin withinside the center of the 2020s. These algorithms can face up to assaults with the aid of using each classical and quantum computer systems and offer a node ahead to the virtual infrastructure safety withinside the quantum era. The evaluation but suggests that troubles of scalability, computation load, and interoperability of those new schemes are being considered mainly in gadgets in resource-restricted networks along with the Internet of Things. Therefore, PQC is an vital factor of countermeasures, however it isn't always a panacea and can't be implemented with out strict implementation strategies.

Besides the post-quantum encryption process, literature calls quantum key distribution (QKD) an influential and in addition to an appealing way of making sure most protection in communication. QKD builds at the foundations of quantum mechanics specially the quantum states crumble upon remark in order that steady cryptographic key trade may be allowed. Practical consequences in China, Europe, and North America have furnished the opportunity of QKD in terrestrial fiber networks or even thru the satellites. Other researchers painting QKD because the cease sport in making sure protection withinside the destiny however a few researchers have pointed at its shortcomings, together with being expensive, restricted in range, prone to side-channel interference, and almost not possible to enforce on a worldwide scale. It is this type of divergence of perspectives that factors to a greater widespread problem of whether or not cybersecurity withinside the quantum age goes to be attained through completely new types of technology on the only hand or reviewed variations of classical structures quantum-resistant in essence at the different.

The dual-use problem of quantum computing is likewise raised withinside the evaluation. Granted the opportunity of creating breakthroughs in drug discovery, substances technology and answer optimization issues, the identical abilities can empower nation and non-kingdom actors in adopting exceptional cyberattacks. The duality creates an extended moral and rule dilemma. The statistics shows that governments are in opposition to broaden quantum supremacy and governments are spending billions of bucks on quantum trends withinside the United States, China, and the European Union. Geopolitics of competing over quantum strength have the ability to offer an imbalanced approach of strength distribution, wherein people with advanced era are dominant withinside the area of cybersecurity as weaker international locations comply with suit. The proposed asymmetries are primarily based totally at the virtual divide formerly skilled for the duration of different technological revolutions, but the virtual divide should have a greater huge effect on present day societies which closely depend on virtual structures. It is right here that the difficulty of a quantum divide consequently involves awareness as a count of issue due to fairness, get right of entry to and compatibility everywhere withinside the world.

The different predominant subject matter is institutional preparedness of the quantum transition. The analyzed reviews and case research suggest that the extent of focus of the quantum risk has improved dramatically, while a huge range of industries have now no longer but taken any steps to make certain that their structures may be transferred to post-quantum cryptography, in particular, financial, healthcare, and authorities industries. The approach of give up-to-quit cryptography infrastructure alternative is slow, expensive, and complex, mainly thinking about the billions of gadgets and networks that function the usage of modern requirements. The trouble with behind schedule adoption is that they'll create a prone important infrastructure to assaults while quantum abilities come into being. Besides, a technical development lag in the back of the coverage preparedness is recognized withinside the evaluation. Although the technical groups like NIST and ETSI are progressing at the requirements of PQC, governance fashions to compel or inspire its usages are nevertheless lower, and there may be no worldwide coordination. Such an imbalance will result in unequal safety elements throughout each sectors and borders, and it enhances the exhilaration of vulnerabilities withinside the interacting virtual ecosystem.

Ethically, the information are indicative of privateness, duty issues and the opportunity of the use of quantum technology for dangerous purposes. Provided that retroactive decryption is feasible with quantum computing, there is probably many years of privateness misplaced in communications and saved records in person and company history. This risk now no longer simplest destroys religion in virtual structures, however might also additionally have dire influences on countrywide protection, commercial enterprise organizational strategy, and man or woman privateness. Also, any other moral issue to the dialogue is can governments and organizations have the ethical responsibility to preempt assaults through quantum computer systems at prohibitive fee withinside the majority of instances to protect residents and consumers? The issue of responsibility is even greater complex in case of viable screw ups of post-quantum cryptographic encryption codes. In case new requirements have vulnerabilities and breaches occur, duty of people withinside the shape of developers, regulating our bodies and implementers may end up debatable.

The different step of evaluation is hooked up with the velocity and the fluctuation of quantum innovation. Whilst different pupils have expressed difficulty approximately an approaching Q-Day wherein the quantum computer systems will render the encryption useless today, a few students have warned towards panic through maintaining that plenty greater engineering needs to be achieved. This ambiguity makes it tougher to make selections in organizations: flow too slowly and chance dealing with the disastrous errors; performing too fast, it's far inevitable funding in untested generation. The literature consequently is reaffirmation of a pressure among urgency and realism which pegs the significance of adaptive regulations consisting of hybrid cryptographic fashions with a mix of classical and post-quantum techniques throughout the transition process.

The records additionally suggest that worldwide cooperation is essential and is as a substitute tough to realize. Since nuclear technology helped create global treaties and non-proliferation links, quantum computing may necessitate a comparable gadget of governing the generation to make sure its abuse is averted even as on the equal time making sure marginalized accessibility. Nevertheless, because of predetermined geopolitical race this is already seen withinside the quantum race, such cooperation is a query of uncertainty. The trouble is a way to strike the proper stability among countrywide safety necessities and the acknowledgment of the fact that cybersecurity in imagining of the quantum technology can virtually be appeared as a international good. Lack of coordination can simplest growth dangers of disjointed answers, absence of consistency and misuse via way of means of horrific elements.

In general, the dialogue well-knownshows that quantum computing isn't always a technical matter, however a exceptionally socio-technical phenomenon with widespread effects. Its personal weaknesses pose threats to undermine the self assurance in virtual infrastructure, and new costs, implementation, and fairness troubles are rising with the improvement of its answers. The moral and geopolitical issues that quantum computing can bring about themselves are doubled over with the aid of using the truth that it's far a dual-use generation that needs similarly innovational answers to governance. Finally, the effects imply that the motives why a destiny this is quantum calls for going past the clinical and engineering innovation would require institutional adaptability, global collaboration, and forward-thinking.

CONCLUSION

Quantum computing is an critical possibility to the destiny of cybersecurity and additionally a huge risk to it. The reality that it may decrypt famous encryption systems, like RSA and ECC, is a trademark that it have to reply urgently with model through post-quantum cryptography and hybrid models. Simultaneously, quantum technology offer protecting technology with brilliant opportunities, greater particularly quantum key distribution that could rework the which means of secure communication. The ubiquitous opposition to make quantum supremacy is having technical however additionally moral and geopolitical implications at the worldwide level, that allows you to require a globalized approach. Although it isn't always clean but as to whilst large-scale quantum dangers can grow to be reality, the smart flow is to put together in advance, put money into research, and feature truthful get admission to to quantum-resilient solutions. Simply put, the shift in the direction of a post-quantum international may be now no longer simplest technological however additionally an ordeal or tribulation as foresight, collaboration, and obligation withinside the procedure of assuring the virtual destiny.

REFERENCES

Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009). Post-quantum cryptography. Springer. https://doi.org/10.1007/978-3-540-88702-7

Boneh, D., & Lipton, R. J. (1995). Quantum cryptanalysis of hidden linear functions. Lecture Notes in Computer Science, 963, 424–437. https://doi.org/10.1007/3-540-60176-2_34

Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on post-quantum cryptography (NISTIR 8105). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

Gidney, C., & Ekerå, M. (2019). How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits. Quantum, 3, 102. https://doi.org/10.22331/q-2019-10-24-202

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38–41. https://doi.org/10.1109/MSEC.2018.053311646

National Institute of Standards and Technology. (2022). Post-quantum cryptography standardization: Round 3 finalists. U.S. Department of Commerce. https://csrc.nist.gov/projects/post-quantum-cryptography

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., … Wallden, P. (2020). Advances in quantum cryptography. Advances in Optics and Photonics, 12(4), 1012–1236. https://doi.org/10.1364/AOP.361502

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

Unruh, D. (2017). Post-quantum security of Fiat–Shamir. In J. Katz & H. Shacham (Eds.), Advances in Cryptology – CRYPTO 2017 (pp. 65–95). Springer. https://doi.org/10.1007/978-3-319-63688-7_3

World Economic Forum. (2022). Quantum computing governance principles: Building a framework for responsible innovation. World Economic Forum. https://www.weforum.org/reports/quantum-computing-governance-principles