https://doi.org/10.48047/AFJBS.6.12.2024.4979-4988

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

Strategies for Securing Quantum Cryptography Systems in the Era of Emerging Technologies

N. Venkata Sai Vivek[1], Sanaka Anuhya [2], Surya Teja Kolli [3], Akhila Donthireddty [4], Solleti Phani Kumar [5]

1Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, India. 2100030375cseh@gmail.com

2Department of Computer Science and Engineering, Koneru Lakshmaiah EducationFoundation, Guntur, India. 2100030476cseh@gmail.com

3Department of Computer Science and Engineering, Koneru Lakshmaiah EducationFoundation, Guntur, India. 2100030519cseh1@gmail.com

4 Department of Computer Science and Engineering, Koneru Lakshmaiah EducationFoundation, Guntur, India. 2100030634cseh@gmail.com

5Department of Computer Science and Engineering, Koneru Lakshmaiah EducationFoundation, Guntur, India. phanikumar.solleti@gmail.com

Article History
Volume 6, Issue 12, 2024
Received: June 10, 2024
Accepted: July 5, 2024
doi:
10.48047/AFJBS.6.12.2024.4979-4988

Abstract-Quantum cryptography is a cutting-edge field that leverages the principles of quantum mechanics to address the inherent vulnerabilities of classical cryptographic systems. This paper provides an overview of the fundamental concepts and protocols that underpin quantum cryptography, highlighting its potential to revolutionize secure communication.The foundation of quantum cryptography lies in the principles of quantum superposition and entanglement, enabling the creation of cryptographic protocols that offer unprecedented levels of security. Key distribution protocols, such as the celebrated BBM92 protocol (BB84), utilize quantum properties to establish secret keys between parties, with the security guaranteed by the no-cloning theorem and the observer effect inherent in quantum systems. Entanglement-based quantum key distribution (QKD) protocols, such as E91, enable secure communication over long distances by exploiting the entanglement of quantum particles. The paper explores the challenges and advancements in the practical implementation of QKD systems, including issues related to quantum channel noise, quantum key distribution over optical fibers, and the development of quantum repeaters.Furthermore, quantum cryptography extends beyond key distribution, with quantum-resistant cryptographic primitives providing a potential solution to the threat posed by quantum computers to classical cryptographic algorithms. Post-quantum cryptography, including lattice-based cryptography and hash-based cryptography, is discussed as a countermeasure to quantum attacks.The paper also delves into the current state of quantum cryptography research and development, highlighting experimental breakthroughs and advancements in quantum communication networks. Quantum key distribution networks and quantum teleportation are explored as potential future avenues for the widespread deployment of quantum-

secure communication.In conclusion, this paper emphasizes the transformative potential of quantum cryptography in ensuring the confidentiality and integrity of communication in the face of evolving technological threats. As quantum technologies continue to advance, quantum cryptography stands at the forefront of the next generation of secure communication protocols, paving the way for a quantum-secure future.
Keywords: Quantum Cryptography, Protocols, Disrupting Operations.

1. Introduction

Breaches are on the rise, and players from academia to businesses to research groups are all potential targets for cyberattacks. cybercriminals, hackers, and even organized groups – are eyeing the valuable secrets and data locked within these fragile systems. [3]Stealing information, disrupting operations, or simply causing chaos. The key is to build security right in from the start, shifting our focus to proactive measures instead of scrambling to fix breaches later. This "Left Shift" in security means thinking about safety like a sturdy foundation, not just an afterthought. This is especially crucial for Quantum Cryptography, where powerful applications are pushing the boundaries of traditional information systems. [4]Integrating security during the design phase of software, hardware, and services ensures that trust and protection are woven into the very fabric of these emerging technologies. we're not just protecting ourselves from tomorrow's attacks – we're building a future where Quantum Cryptography can thrive, unlocking its incredible potential without fear of falling prey to malicious actors. It's time to turn our house of cards into a secure fortress, ready to face the challenges and opportunities of the Quantum era.

The world's gone digital, and our data, from medical records to company secrets, gallops through cyberspace on virtual horses. [11]But just like the Wild West, this vast online frontier has its outlaws: cybercriminals, hackers, and even nation-states with their digital six-shooters. And their target? Anything valuable, especially the sensitive data stored by companies, universities, and research groups. Think of these entities like gold mines brimming with intellectual property, research findings, and cutting-edge technological secrets. A juicy target for digital bandits looking to steal valuable nuggets or disrupt operations with a well-placed cyber-dynamite. [9]Recent attacks on supercomputers, universities, and R&D labs show just how real this threat is. Imagine a hacker hijacking a crucial medical database, holding sensitive patient information hostage. Or a cyber-attack crippling a power grid, plunging entire cities into darkness. These are the chilling possibilities in our increasingly digital world. Enter Quantum Cryptography Security – the brave marshal riding to the rescue. It's all about building strong virtual walls and deploying digital posses to protect our data from these modern-day outlaws. [22]This isn't just a concern for tech giants. Startups, university spin-offs, and even small businesses with innovative ideas are potential targets. That's why discussions about Quantum Cryptography Security are crucial, not just for securing existing technologies but also for building strong defences into future software and hardware. Imagine Quantum Cryptography as a brand-new gold rush town. Everyone's scrambling to stake their claim, but before we build anything, we need to establish ground rules and safety measures. That's what this survey aims to do – spark dialogues, brainstorm ideas, and pave the way for interdisciplinary research in Quantum Cryptography Security. By nurturing talent and fostering collaboration, we can create a safer, more secure digital world for everyone.

Before we explore how systems can be threatened, let's grasp some basics about quantum computers. These systems blend different parts to make a special processor that uses quantum effects in cryptography. According to Amdahl's Law, adding a co-processor to a central processing unit can speed up overall execution, especially for tough tasks, making it an accelerator. To be fully capable, a quantum processing unit (QPU), acting as the co-processor, needs a way to convert analogue signals between the control system and the application logic, which is done through an analogue-to-digital interface. Also, a Host-CPU is needed to connect

to a network. Figure 1 gives an example of what a typical quantum accelerator looks like. For example, Quantum as a Service (QaaS) lets you access cryptography power when you need it, like through the cloud or other remote methods

2. Literature Survey

Those days might be coming to an end. While we still squeeze incredible progress out of technology, things like clock speeds and efficiency gains are slowing down. We're hitting fundamental limits with the way we build things. Picture it like shrinking buildings on a shrinking street. [5]Laws like Moore's Law (smaller transistors = faster chips) and Koomey's Law (lower energy use) are our street grid, but the buildings (circuits) can only shrink so much before they run into walls like the Landauer limit (information costs energy). This is where Quantum Cryptography steps in. It's like a whole new street network, bypassing the old limitations. But it's also under construction. Quantum Processing Units (QPUs) are still young, needing regular tune-ups and downtime, like fixing potholes and rerouting traffic. Plus, some key pieces are missing, like real Quantum Random Access Memory (QRAM). [6]Most QPUs today only have "read-only" memory, like road signs, not stoplights. So, while Quantum Cryptography shines like a promising future city, it's still got construction cones and detours. But the potential is mind-blowing, opening up possibilities we can't even imagine with our current tech. And that's why, despite the challenges, we're excited to explore this new frontier of cryptography.

For decades, we've zoomed along the tech highway, constantly upgrading to faster processors and slicker software. But lately, it feels like we're stuck in rush hour. Moore's Law, the guiding principle of miniaturization and faster chips, is hitting a red light. [7]Even though we're still making progress, fundamental limits like Koomey's Law (energy efficiency) and Denard's Law (power dissipation) are acting like roadblocks. Think of it like trying to shrink your car on a shrinking street – eventually, you hit walls like the Landauer limit, where information itself requires energy to process.

We take a quantum leap onto a whole new freeway – Quantum Cryptography. It's like an entire parallel network, bypassing the old rules and limitations. But this new highway is still under construction. Quantum Processing Units (QPUs), the engines of this quantum world, are young and finicky. [17]They need regular maintenance and calibration, like pit stops and detours. Quantum Random Access Memory (QRAM), the crucial "read-write" storage system. Right now, most commercial QPUs only have Read-Only Memory (QROM), like highway signs without traffic lights. It's a one-way street, limiting their potential. But like engineers working on innovative solutions, researchers are tirelessly exploring ways to build robust QRAM and unlock the full power of this quantum superhighway. There are bumps along the quantum road, but the potential is mind-boggling. From cracking complex codes to revolutionizing materials science, the possibilities are like unexplored scenic routes waiting to be discovered. So, even with the detours and challenges, we're excited to navigate this new era of cryptography. It's not just about pushing faster clock speeds, it's about exploring entirely new roads to unleash the incredible power of quantum mechanics. Imagine simulating entire proteins, designing custom drugs that fit our bodies like a glove, or creating revolutionary materials with never-before-seen properties. These mind-boggling possibilities drive the development of Quantum Cryptography, not hacking sprees. But these "super microscopes" are still under construction. We're in the kindergarten stage, with a long way to go before they challenge your laptop's password protection. [20]Headlines about cracking RSA encryption,Quantum Cryptography devices are like toddlers compared to the powerhouses needed for such feats. Estimates suggest millions of tiny "quantum bits" would be needed, and we're barely at the hundred mark.

Theoretical ideas about cracking encryption exist, but they're just that – theories. Building practical tools based on them is like baking a cake from a recipe scribbled on a napkin.

[17]Even if we achieved faster key searches with the famous Grover algorithm, it wouldn't break encryption used in things like online banking. Today's supercomputers wouldn't even budge against something like AES-256 encryption. it's true that shorter key lengths smaller than AES-256 might be vulnerable in the future. [18]Think of them as bicycle locks instead of bank vaults – easier to crack if quantum advancements reach a certain point. So, it's crucial to stay ahead of the curve and update encryption standards as Quantum Cryptography evolves. Quantum Cryptography is about unlocking scientific miracles, not cyber crimes. It's about designing life-saving drugs, understanding the universe at its core, and maybe even creating materials that bend light or teleport data. Let's focus on harnessing its power for good, while keeping a watchful eye on potential security challenges as this exciting field unfolds

3. Methodology

Building a secure cyber fortress isn't about slapping on the biggest, fanciest locks. It's about knowing your walls, understanding the terrain, and strategically placing defences where they matter most. Understanding how your systems and applications interact is crucial for identifying potential vulnerabilities. Peek over the ramparts and assess the surrounding environment. Is it a bustling digital marketplace or a quiet countryside manor? Different landscapes require different levels of security. You wouldn't build a gold-plated moat around a thatched hut, so be realistic about your budget and available skills. Striking a balance between cost and security is key. A good defence doesn't have to be the most expensive, but it should be tailored to your specific needs. The final step is figuring out the threats. Once you've got this information, you can start building your defences. It's a layered approach, like a castle with moats, drawbridges, and strong walls. Think firewalls, intrusion detection systems, and vigilant guards. By prioritizing essential measures based on the identified risks, you can create a robust and cost-effective security posture. your cyber fortress is never truly finished. Threats evolve, technology changes, and the landscape shifts. Continuously assessing, adapting, and upgrading your defences is key to keeping your digital treasures safe.

4. A Quantum Key Distribution Example

In the ever-evolving landscape of cyber threats, building a strong defence is no longer an option, it's a necessity. Just like a medieval fortress, our digital systems require well-maintained walls, vigilant guards, and robust protocols to repel unwelcome attacks. This document examines key strategies for bolstering your cybersecurity posture, particularly in the context of Quantum Cryptography systems. The foundation of any strong defence lies in good hygiene and awareness. This starts with instilling a culture of cyber safety within your organization. Regular training programs can educate employees on best practices like strong passwords, phishing awareness, and secure cloud usage. Implementing multi-factor authentication adds an extra layer of protection, making it harder for attackers to breach logins even with stolen credentials. With the rise of remote work and cloud migration, the traditional fortress perimeter has eroded. Now, endpoints like laptops and home networks become potential weaknesses. Implementing endpoint protection software, encrypting data both at rest and in transit, and employing robust firewalls are crucial safeguards. Hybrid and cloud architectures, while offering immense flexibility, require careful configuration. Implementing segmentation, authorization, authentication, and encryption measures ensure that even if one part of the system is compromised, attackers cannot easily move laterally and access sensitive data. Depending on your risk tolerance and the criticality of your assets, adopting a zero-trust security model may be the most secure option.

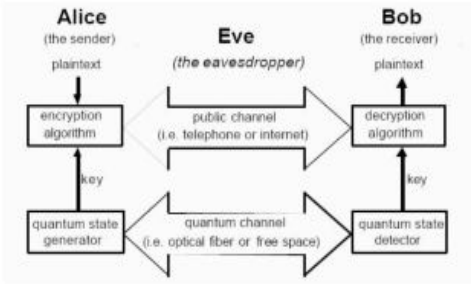

Figure 1. Quantum Key Distribution

Quantum Key Distribution Example

Non-production environments, including research and development systems, often receive less attention but remain vulnerable. Regularly updating software and migrating from outdated protocols like OPC Classic in Industrial Control Systems (ICS) to newer, more secure options like OPC UA are crucial steps. Segmenting these systems and implementing robust access controls, along with firewalls and DMZs when applicable, further strengthens your overall security posture. Quantum Cryptography systems present unique challenges due to their combination of off-the-shelf components and proprietary software and hardware. This underscores the importance of secure design practices throughout the development process, particularly for commercially available systems. Releasing source-code bug fixes promptly is vital, and organizations must remain proactive in identifying and addressing vulnerabilities in their own software and the off-the-shelf components they utilize. Regular monitoring for security patches and updates is essential to stay ahead of potential exploits. it's a continuous journey of vigilance and improvement. By prioritizing good cyber hygiene, raising awareness amongst your team, and implementing robust security measures across your entire digital landscape, you can establish a strong first line of defence against cyber threats, even in the face of emerging technologies like Quantum Cryptography. Remember, a secure digital fortress is built brick by digital brick, requiring constant upkeep and adaptation to remain impregnable.

5. QDKProtocols Implementations

The critical systems that control our world, from power grids to industrial plants, rely on complex computer networks known as Control Systems. Just like medieval castles with multiple lines of defence, these systems need robust safeguards to withstand modern cyberattacks. This document explores key strategies for fortifying the security of these vital networks, particularly in the context of Quantum Cryptography Systems and Industrial Control Systems (ICS). Imagine a castle with only one drawbridge – attackers need only conquer it to gain access. Similarly, control systems often have "single points of failure," vulnerabilities that, if exploited, could cripple the entire system. One crucial method to combat this is segmentation. Picture multiple drawbridges leading to different sections of the castle – even if one falls, the others remain intact. In Quantum Cryptography Systems, for example, segmenting the fail-safe cooling system from the control unit of the Application Development Interface/Quantum Processing Unit (ADI/QPU) ensures that a compromised Host-CPU cannot trigger both a temperature rise and seize control, potentially causing disastrous malfunctions.

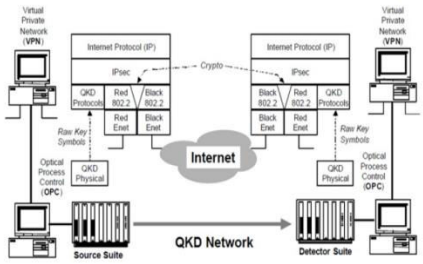

Figure 2. QDK Protocols Implementations

Unlike digital fortresses, control systems often involve human interaction. In an air-gapped ICS, where the network is physically isolated from the internet, the biggest vulnerability becomes the physical gap itself. Unauthorized access by disgruntled employees or unsuspecting workers can compromise even the most secure system. Therefore, strict physical access controls, whitelisting of approved USB devices, and mandatory device antivirus scans are crucial for mitigating insider threats and unwitting security lapses. Organizations responsible for critical control systems are not alone in their fight against cyber threats. Established frameworks like SANS CIS Controls and MITRE Shield offer comprehensive guidelines for securing systems against specific attack tactics. Tools like OPC ICS Security Tools assist in designing and implementing secure OPC systems, while resources like OWASP's CLASP and Microsoft's SDL guide software developers in identifying and correcting vulnerabilities throughout the entire design and development process, ensuring security is woven into the very fabric of the software.

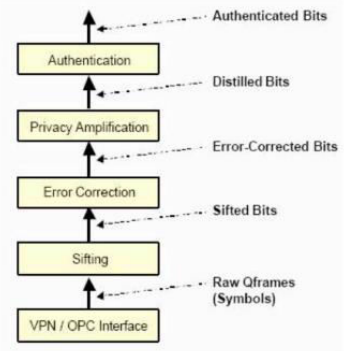

Figure 3. QDK Protocol Stack

QKD Protocol Stack

Taking security a step further is the DevSecOps framework. Imagine a castle where skilled artisans build every stone with defence in mind – DevSecOps integrates security tools and processes throughout the software development lifecycle, from the initial design stages to deployment and maintenance. Developers can utilize tools like Metasploit and W3AF to proactively test their software for vulnerabilities, effectively patching any weak spots before they can be exploited. Securing control systems is a continuous endeavour, requiring vigilance and active adaptation. By implementing diverse strategies like segmentation, fail-safe systems, robust access controls, and leveraging readily available resources and tools, organizations can build digital fortresses capable of repelling even the most sophisticated cyberattacks. Remember, strong control systems are not built overnight – they are the result of meticulous planning, constant vigilance, and a commitment to integrating security into every aspect of their operation. In this way, we can ensure that the critical systems that power our world remain resilient in the face of ever-evolving cyber threats.

6. Conclusion

Standing at the threshold of a groundbreaking era, Quantum Cryptographypromises solutions to problems once deemed impossible. This potential, however, comes nestled within a landscape of unprecedented complexity and potential vulnerability. Limited resources, cutting-edge technology, and ever-evolving threats necessitate a decisive shift in security paradigms. It's not enough to simply build the Quantum City – we must fortify it from the ground up. Picture a city built on sand, shimmering with architectural marvels yet prone to crumble under the slightest tremor. The nascent Quantum City must not follow this path. Security cannot be an afterthought – it must be a foundational pillar, woven into the very fabric of both hardware and software components. Every circuit, every line of code, every quantum qubit must be designed with inherent security features, acting as robust shields against potential attacks and unintentional vulnerabilities. This isn't paranoia, it's prudence – a proactive approach that mitigates risks before they manifest, ensuring the city's future thrives on innovation, not exploitation.

A secure city thrives on awareness. Imagine a network of vigilant citizens sharing whispers of suspicious activity – this is the essence of threat intelligence platforms like MISP in the quantum realm. By fostering collaboration and information sharing, organizations gain critical insights into the tactics and motivations of malicious actors. MISP becomes a crystal ball, revealing emerging threats before they materialize, allowing defences to be pre-emptively strengthened. It's a collective shield, protecting not just individual systems but the entire Quantum City, ensuring no shadowy figure can operate unseen. The spectre of sabotage, espionage, and extortion looms large over this new frontier. Imagine competitors sabotaging groundbreaking experiments, stealing invaluable research data, or holding critical calculations hostage. This necessitates robust access controls, stringent data encryption protocols, and thorough vetting of personnel at all levels. Every citizen within the Quantum City must be accountable, aware of their role in maintaining security and vigilant against potential threats. It's a city where trust is paramount, where every line of code, every access point, every human interaction contributes to a secure and resilient ecosystem.

Securing the future of Quantum Cryptography is not a solo act. It's a symphony of collaboration, a global chorus where researchers, developers, governments, and security experts harmonize their efforts. Open communication, shared knowledge, and collective investment in robust safety measures are the instruments that will orchestrate resilience. Imagine a city council, diverse in expertise and united in purpose, working tirelessly to safeguard its citizens. This is the spirit that must guide us – a recognition that the Quantum City thrives on shared responsibility, where every innovation, every line of defence, strengthens the whole. The potential of Quantum Cryptography is boundless, but this potential can only be realized on a foundation of robust security. By adopting a proactive approach that prioritizes security from the ground up, leverages the power of threat intelligence, and fosters a culture of collaboration, we can build a Quantum City that is not just innovative, but also safe and trustworthy. Let us ensure that the brilliance of this new technology isn't dimmed by vulnerabilities, but rather shines with the clarity of foresight and proactive defence. Together, we can unlock the incredible potential of Quantum Cryptography while safeguarding it from the shadows, paving the way for a future where innovation thrives alongside trust, and the Quantum City stands tall, a testament to our collective ambition and foresight.

References

[1] CrowdStrike, 2021 global threat report: Adversary trends and analysis, Accessed: 2021. URL: https://www.crowdstrike.com/resources/reports/global-threat-report/.

[2] Bitdefender, Cyberattack against uk supercomputer archer forces operators to disable access for scientists, Accessed: 2021.

URL: https://www.bitdefender.com/blog/hotforsecurity/ cyberattack-against-uk-supercomputer-archer-forces-operators-to-disable-access-for-scientists.

[3] J. News, Forschungszentrumjülich - jsc - archiv newsletter "jsc news" - cyberattack against supercomputers, Accessed: 2021.
URL:https://www.fz-juelich.de/SharedDocs/Meldungen/ IAS/JSC/EN/2020/2020-06-cyberattack.html?nn=1060464.

[4] NCSC, More ransomware attacks on uk education - ncsc.gov.uk, Accessed: 2021.URL: https: //www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector.

[5] N. Dunn, An introduction to quantum cryptography for security professionalsauthor, 2021.

[6] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, D. Smith-Tone, Report on post-quantum cryptography, 2016.
URL: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR. 8105.pdf. doi:10.6028/NIST.IR.8105.

[7] D. Moody, G. Alagic, D. C. Apon, D. A. Cooper, Q. H. Dang, J. M. Kelsey, Y.-K. Liu, C. A. Miller, R. C. Peralta, R. A. Perlner, A. Y. Robinson, D. C. Smith-Tone, J. Alperin-Sheriff, Status report on the second round of the nist post-quantum cryptography standardization process, 2020.
URL: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf. doi:10. 6028/NIST.IR.8309.

[8] A. Majot, R. Yampolskiy, Global catastrophic risk and security implications of quantum computers, Futures 72 (2015) 17–26. doi:10.1016/J.FUTURES.2015.02.006

[9] Q. Flagship, Competence framework for quantum technologies compiled by franziskagreinert and rainermüller version 1.0 (may 2021), 2021. URL: https://op.europa.eu/en/ publication-detail/-/publication/93ecfd3c-2005-11ec-bd8e-01aa75ed71a1/language-en.

[10] A. Reuther, P. Michaleas, M. Jones, V. Gadepally, S. Samsi, J. Kepner, Survey of machine learning accelerators (2020).
URL: http://arxiv.org/abs/2009.00993http://dx.doi.org/10.1109/ HPEC43674.2020.9286149. doi:10.1109/HPEC43674.2020.9286149.

[11] K. Bertels, A. Sarkar, A. Krol, R. Budhrani, J. Samadi, E. Geoffroy, J. Matos, R. Abreu, G. Gielen, I. Ashraf, Quantum accelerator stack: A research roadmap (2021).
URL:http: //arxiv.org/abs/2102.02035.

[12] T. N. Theis, H. S. P. Wong, The end of moore's law: A new beginning for information technology, Cryptography in Science and Engineering 19 (2017) 41–50. doi:10.1109/MCSE. 2017.29.

[13] M. Horowitz, 1.1 cryptography's energy problem (and what we can do about it), Digest of Technical Papers - IEEE International Solid-State Circuits Conference 57 (2014) 10–14.
doi:10.1109/ISSCC.2014.6757323.

[14] R. Landauer, Irreversibility and heat generation in the cryptography process, IBM Journal of Research and Development 5 (2010) 183–191.
doi:10.1147/RD.53.0183.

[15] O. D. Matteo, V. Gheorghiu, M. Mosca, Fault tolerant resource estimation of quantum random-access memories (2020).

[16] J. Preskill, Quantum cryptography in the nisq era and beyond, Quantum 2 (2018) 79. doi:10.22331/q-2018-08-06-79.

[17] M. Sarovar, T. Proctor, K. Rudinger, K. Young, E. Nielsen, R. Blume-Kohout, Detecting crosstalk errors in quantum information processors, Quantum 4 (2020) 321.

URL: https: //quantum-journal.org/papers/q-2020-09-11-321/. doi:10.22331/q-2020-09-11-321.

[18] S. J. Pauka, K. Das, R. Kalra, A. Moini, Y. Yang, M. Trainer, A. Bousquet, C. Cantaloube, N. Dick, G. C. Gardner, M. J. Manfra, D. J. Reilly, A cryogenic cmos chip for generating control signals for multiple qubits, Nature Electronics 2021 4:1 4 (2021) 64–70.
URL:https: //www.nature.com/articles/s41928-020-00528-y. doi:10.1038/s41928-020-00528-y.

[19] C. Gidney, M. Ekerå, How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits (2019). URL: http://arxiv.org/abs/1905.09749http://dx.doi.org/10.22331/ q-2021-04-15-433. doi:10.22331/q-2021-04-15-433.

[20] IBM, Ibm's roadmap for scaling quantum technology | ibm research blog, Accessed: 2021.
URL: https://research.ibm.com/blog/ibm-quantum-roadmap.

[21] Élie Gouzien, N. Sangouard, Factoring 2048-bit rsa integers in 177 days with 13 436 qubits and a multimode memory, Physical Review Letters 127 (2021).
doi:10.1103/ physrevlett.127.140503.

[22] L. K. Grover, A fast quantum mechanical algorithm for database search, Proceedings of the Annual ACM Symposium on Theory of Cryptography Part F129452 (1996) 212–219.
URL: https://arxiv.org/abs/quant-ph/9605043v3.

[23] J. Tibbetts, Quantum cryptography and cryptography: Analysis, risks, and recommendations for decisionmakers, 2019.

[24] S. INstitute, Sans ics control systems are a target v1.3 09.30.21.pdf, Accessed: 2021.
URL: https://sansorg.egnyte.com/dl/j2o3K3iiPy.

[25] Fortinet, Cloud security report (2021). URL: https://www.fortinet.com/content/dam/ fortinet/assets/analyst-reports/ar-cybersecurity-cloud-security.pdf.

[26] OAWSP, Owasp top ten web application security risks | owasp, Accessed: 2021.
URL: https://owasp.org/www-project-top-ten/.

[27] Kaspersky, Threat landscape for industrial automation systems. statistics for h2 2020 | kasperskyics cert, 2021.
URL: https://ics-cert.kaspersky.com/reports/2021/03/25/ threat-landscape-for-industrial-automation-systems-statistics-for-h2-2020/.

[28] Dragos, The ics threat landscape (2019).
URL: https://www.dragos.com/wp-content/ uploads/The-ICS-Threat-Landscape.pdf.

[29] CWE, Cwe - 2021 cwe top 25 most dangerous software weaknesses, Accessed: 2021.
URL: https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html.

[30] MITRE, Mitreattck® matrix for enterprise, Accessed: 2021.
URL:https://attack.mitre.org/ matrices/enterprise/.

[31] MITRE, Attck® for industrial control systems, Accessed: 2021.
URL:https://collaborate. mitre.org/attackics/index.php/Main_Page.

[32] S. Institute, Cis controls v8 released | sans institute, Accessed: 2021. URL: https://www.sans.org/blog/cis-controls-v8/.

[33] MITRE, Active defense matrix, Accessed: 2021.
URL: https://shield.mitre.org/matrix/.

[34] Github, Ics-security-tools/pcaps/opc at master · iti/ics-security-tools · github, Accessed: 2021.
URL: https://github.com/ITI/ICS-Security-Tools/tree/master/pcaps/OPC.

[35] CLASP, The clasp application security process the clasp application security process introduction 1 (2005).

[36] Microsoft, Microsoft security development lifecycle, Accessed: 2021. URL: https://www. microsoft.com/en-us/securityengineering/sdl/.
[37] S. Pratte, S. Fortozo, G. Kispal, A. Banvait, A. Azazi, N. Hiebert, Strategies for secure software development (2013).
[38] MISP, Misp galaxy clusters misp galaxy cluster (2021). URL:https://www.misp.software/galaxy.pd