Quantum Signal Processing: Strengthening Cyber Defense

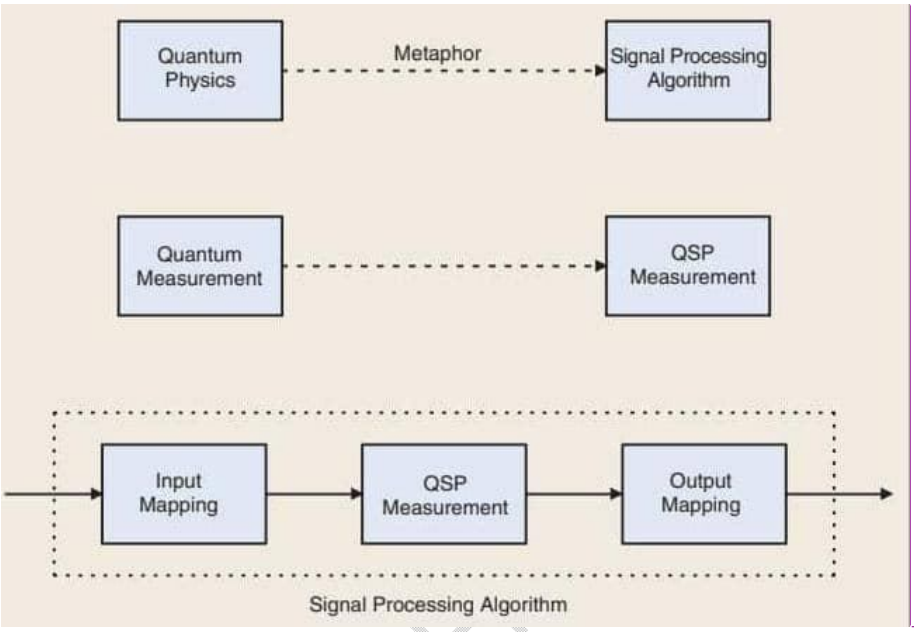
ABSTRACT

Aim: To examine the strengthening of cyber defense using Quantum Signal Processing. **Significance of Study:** There is need for the application of Quantum Signal Processing in cyber security due to the vulnerable attack. This paper addresses the relevant issues on the use of Quantum Signal Processing in strengthening cyber defense. **Problem Statement:** The development of cyber space and its inestimable contribution in information dissemination has led to its wide patronage and usage. Thus, third party are intruding to hijack and hack secretive information to suite their own purpose. **Discussion:** The concepts of Quantum Signal Processing and cyber defense were examined. The measurement consistency principle, measurement concept and quantization of the measurement output principle were identified as the three interconnected fundamental principles of quantum mechanics in Quantum Signal Processing. The existing correlation between QSP framework and quantum physics together with relevant key results were also examined. was also discussed with major Considerations were given to modification of known algorithms, measurement parameters utilization, probabilistic mappings, imposition of inner product constraints and oblique projections as the algorithm design in quantum signal processing framework. **Conclusion:** In conclusion, Quantum Signal Processing is applicable in strengthening cyber defense.

Keywords: Quantum Signal Processing, Cybersecurity, Quantum Computing, Algorithm, Cyber Defense

1. INTRODUCTION

Quantum Signal Processing (QSP) framework is a function of (1)measurement, (2) consistency concepts and (3) quantization based on quantum systems. Also, QSP simplifies and adopts the inner product restriction, specifically orthogonality that quantum physics implements on measurement of vectors. However, the QSP framework broad and unlimited more than the quantum measurement framework. This resulted from the absence of constraint in the design of the algorithms with respect to the physical quantum mechanics restrictions. The measurements performance is an important factor used in processing systems under quantum mechanics [1]. An algorithm attached to the signals is applied in processing the signal.In order to utilizequantum physics formalism in the design of algorithms and the rich mathematical structure, it is essential to first draw a parallel between a quantum mechanical measurement and a signal processing algorithm through the connection of a signal processing measurement with a signal processingalgorithm. Thequantum measurement formalism and fundamental principles is then connected to the QSP measurement description. An algorithm description via a QSP measurement is carried out in addition to input and output mappings if appropriate [2]. Figure 1 displays the conceptual QSP measurement framework.



Comment [hy1]: Quality of this figures are bad

Figure 1: Conceptual QSP measurement framework

The QSP framework is primarilyassigned with the quantum physics constraints, QSP measurement design, a quantum measurement, borrowing from the principles, and axioms. The QSP measurement depends on some certainset of measurement parameters so as to ensure that this framework provides anessential and suitable setting in order to derive new algorithms through borrowing from varied measurement parameters selection and the ideas of quantum mechanics. Furthermore, the mathematical limits imposed by physics on quantum measurement can equally be imposed on the QSP measurement leading tofascinatingprocessing of new signal algorithms since the QSP measurement is planned to have a mathematical pattern analogous to a quantum measurement[3].

The measurement concept, the measurement consistency principle and measurement output quantization principle are the QSP activeinterrelated fundamental principles of quantum. Additionally, other principles like inner product constraints are entertained when quantum systems are adopted in a communication context. QSP depends on the exploitation of these differentprinciples and constraints based on signal processing algorithms [4]. In the real world, terms such as measurement, measurement consistency and output quantization are well known in signal processing, although not exactly like constraints and mathematical interpretation with reference to quantum mechanics [2]. Allotment ofdifferent imprecise or precise interpretations to measurement can be experienced in signal processing. Measurement has a precisedefinition when quantum mechanics sets in and a lot of them are applied to the QSP framework. In the same way, quantization is conventionallyapplied in fairly particular terms in signal processing. In quantum mechanics, quantization of measurement output is an essential basic principle, and the application of this principle together with the quantum mechanical consistency and measurement notions leads to

potentially interestingsimplifications of quantization as it is normallydetected in signal processing [5].

Consistency of measurement also possess a definite meaning in quantum mechanics. It was exactlyindicated that repeated uses of a measurement must produce equal outcome. The foundation for many algorithms classes such assignal estimation, interpolation and quantization methods is a similar consistency concept when signal processing becomes important [6]. The inter symbol interference escaping condition in waveforms for modulation of pulse amplitude andfilter design interpolation condition are specific early consistencyillustrations that arose classically in signal processing. Additional modernoccurrences are perfect reconstruction filter banks, wavelet approximations and multiresolution, and sampling methods in which the perfect reconstruction condition is exchanged for the less rigorous consistency constraint. Also, the observation of measurement consistency in a wider framework inspired by quantum mechanics can lead to some fascinating and original signal processing algorithms [5].

In the form, a normalized vector is usually applied in the classification of a quantum system. Evidence regarding a quantum system is obtained throughexposing the system to a quantum measurement. A quantum measurement is a probabilistic nonlinear mapping which can be explained in the easiest form with respect to a set of measurement vectors which span measurement subspaces [3]. The laws of quantum mechanics impose the restriction that the vectors must be linearly independent and orthonormal. A measurement of this form is referred to as a rank-one quantum measurement. In an additional overallsituation, the quantum measurement is offered with respect to a set of projection operators onto subspaces where the projections must constitute a whole set of orthogonal projections via quantum mechanics laws. Such a measurement is called subspace quantum measurement [7]. A measurement outcome is intrinsically probabilistic in quantum mechanics. The possibilities ofany measurement outcomes depends on the vector indicating the system original state at the measurement time. The measurement breakdowns the quantum system condition onto the one that is pleasant with the measurement outcome. Generally, the system final condition is not the same as the system condition before the measurement. Consistency of measurement is the basicquantum mechanics postulate, i.e., recurrent measurements on a system must generate the same outcomes; otherwise the measurement output cannot be ascertained [8]. Thus, the system condition after a measurement must be in a way that if the system is re-evaluatedsuddenly in this state, then the final condition after this second measurement will be the same as the condition before the first measurement.

Measurement outcome quantization is a direct consequence of the consistency condition. Precisely, the consistency requirement leads to a class of conditions being referred to as the determinate measurement conditions. These systems are quantum conditions through which the measurement generates a clear outcome with excellent possibility and are the conditions that are positioned entirely in one of the measurement subspaces [9]. Additionally, quantization of thesystem to one of these statesafter the execution of system measurement is carried out despite the system state not being among the determinate states. This denotesthe certainty of system quantization to be part of one of these states in which the possibility of being in a certain determinate state is controlled by the inner products between the system state and determinate [10]. Figure 2 shows the framework of QSPconnection to quantum physics and important key results.

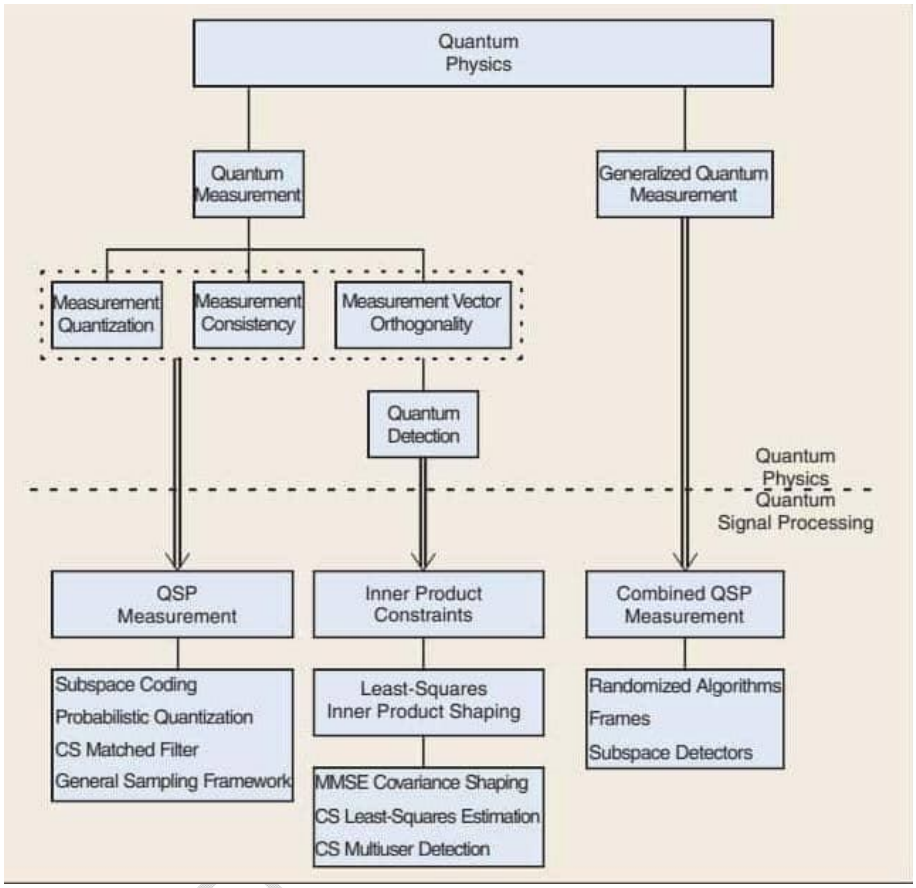


Figure 2: QSP framework connected to quantum physics and relevant key results

.

However, the utilization of QSP as an effective methodology of cyber-attack defense in order to ensure effective cyber security is becoming significant. Previously, internet detection has been contributory to the improved performance of usual human activities that are related to it. Recently, tractable records of speedy improvement in communication technologies have been noticedresulting in the survival of hyper-connected societies leading to a paradigm shift in communication routes from outdated to recent conditions [11]. This over reliance on communications with the aid of internet in executing vital assignments using hyper-connected paradigm demands for information security and privacy before being communicated. An unprotected hyper-connected programmed system can lead todisaster beyond the organization using it. This can be catastrophic if the cyber-world becomes vulnerable to attack. Cyber defense is basically the potential to manage any kind of damage to electronic communication systems and services through information protection involved alongside with its confidentiality, availability, integrity,authentication and non-repudiation maintenance. Cybersecurity involves the practicing of numerous layers of protection in the

entire networks and systems to prevent attacks on mild information and business operations according to CISCO[12].

2. DESIGN OF ALGORITHM IN THE QUANTUM SIGNAL PROCESSING FRAMEWORK

The measurement of QSP is vigorously involved in signal processing of algorithms design with reference to QSP framework. In this framework, the processing of signals occur through the use of some QSP measurement variables or exposing them to a QSP measurement. This is not attained through direct use of the measurement. In order to design an algorithm with the aid of QSP measurement, it is vital todetectthe measurement vectors in a ROM or the projection measurement operators first in a subspace. QSP measurement states the likely measurement outcomes [6]. For example, in a detection case, the transmitted signals may be identical tothe measurement vectors or may represent these signals in a probably different space. In another scenario involving a scalar quantizer, the measurement vectors may be chosen as a set of vectors that denote the scalar quantization levels. In a subspace QSP measurement, the projection operators of the measurement through projections on a set of subspaces are adopted for signaling. The measurement vectors is then inserted [8].

The signal is mapped into another signal through mapping process if the signal to be processed does not fall within. To attain the algorithm output, the execution of the intended signal representation measurement to be processed occurs. Assuming$x$ is a determinate signal of M, this implies that the measurement outcome is related thus: $y = M(x) = x$. Otherwise x is estimatedusing a determinate signal $y$with the aid of a mapping . If suitable, mapping of y (measurement outcome) to the algorithm output can be executed. The choice of variousinput and output mappings; and kinds of measurement variableswith the aid of QSP measurement framework as shown in Figure 3 leads to the arrival at a variation of new and interesting processing techniques [13].

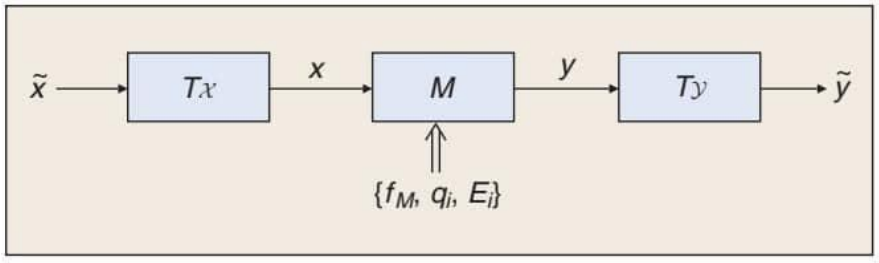


Figure 3: Algorithms Design with the aid of a QSP measurement

2.0.1 MODIFICATION OF KNOWN ALGORITHMS

Many traditional processing and detection techniques are naturally appropriatefor the framework illustrated as Figure 3. Examples are multiuser detection, traditional and dithered quantization, sampling methods and matched-filter detection. Modifications and extensions

of algorithm can be realized through changing of measurement variables if the algorithm is presented in QSP measurement form.

Based on this, the QSP framework provides a unified conceptual structure for numerous techniques involving traditional processing and a precise mathematical setting for creating potentially operative, efficient and new processing routes through measurement parameters modification. It is essential that the algorithm is initially casted like a QSP measurement so as to restructure the algorithm that is existing already and denoted by a mapping via the use of QSP framework[14]. An output mapping and an input mapping are selectedalongside the measurement variables if they are essential. Some of the variables are systematically alteredleading to restructuring of measurement that can then be transformed into a new signal processing algorithm signified by a mapping. The considered modifications arose from either the subdue of some of these limits which are not forced in signal processing or forcing of some quantum mechanics additional restrictions on the parameters measurement. Figure 4 represents the required fundamental steps of QSP measurement for the modification of existing signal processing algorithms. Typical modifications of the parameters examined areinner product constraints imposition on the measurement vectors and adopting probabilistic mapping [8].

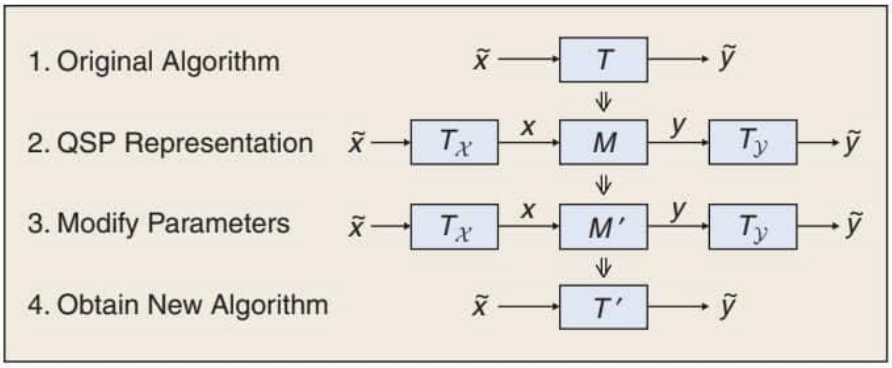


Figure 4: Fundamental steps of QSP measurement for existing signal processing algorithms modification

2.0.2 Utilization of Measurement Parameters

Another type of developed algorithms arose from processing of signal using some measurement parameters together with quantum mechanical constraints imposition directly on these parameters. A common example is seeing any linear signal processing as processing with a set of measurement vectors and product constraints are forced on these vectors. Using quantum detectionideas, linear algorithms can then be designed in a way that they are at maximum level based on these inner product constraints [11]. The algorithm is identified and stated as processing by one of the measurement parameterso as to generate new parameters or adjust existing algorithms.Thus, parameters modification is in accordance with one of the three modifications earlier outlined.

2.0.3 Probabilistic Mappings

Naturally, the QSP framework causesprobabilistic and randomized algorithms through probabilistic mapping which imitates the quantum measurement. This idea can be incorporated in the quantization context. However, the totalpossible advantages of probabilistic algorithms in general resulting from the QSP framework hold an exciting area for future investigations [10].

2.0.4 Imposition of Inner Product Restrictions

One of the significant habits of quantum mechanics is that the measurement vectors are restricted to be orthonormal. This restrictionallows some remarkableencounters such as the quantum detection difficulty. The basic challenge in quantum mechanics is to construct excellent measurements based on this constraint that is most suitable for a known set of state vectors. In the same way to quantum mechanics, an importantfeature of QSP is that of forcing particular kinds of restrictions on algorithms. The QSP framework provides a systematic technique for forcing such constraints [15]. The measurement vectors are restricted to have a specific inner product pattern, as in quantum mechanics. However, since there is no constraint by physical laws, there is no limitation to an orthogonality limit. As part of the QSP framework, the selection techniques for the most suitable set of measurement vectors to describe the signals of interest and have a particular inner product pattern can be created. These techniques are functions ofideas and results received in the perspective of quantum detection, which unlike QSP are function to the quantum physics constraints.

Definitely, measurement vectors are built with a given inner product configuration closer to LS sense of a known set of vectors in a way that the vectors are chosen to minimize the total squared norms of the error vectors. These techniques are referred to as LS inner product shaping. Additional explanations on LS inner product shaping are briefly stated in “Least Squares Inner Product Shaping.” The theory of LS inner product shaping can be acquired to improve efficient solutions to numerousobstacles that originated from the imposition of a deterministic or stochastic inner product limitation on the algorithm and then planningbest algorithms based on this constraint. In each of these obstacles, the algorithm is described as either a QSP measurement which force an inner product limitation on the corresponding measurement vectors or considered as linear algorithms on which the inner product limitations can be forced directly. The imposition of such limitations together with LS inner product shaping causes new processing methods in different areas such as detection, linear estimation, frame theory, covariance shaping and multiuser wireless communication, which usually displaybetter performance over traditional techniques [10].

2.0.5 Oblique Projections

The quantum mechanics rules enforce the limitation on orthogonal projections in a quantum measurement structured with a set of projection operators. Oblique projections may be implored in QSP having more general measurements categories that are well-stated by projection operators who are unlimited to be orthogonal, An oblique projection is a type in which operator E is not essentially Hermitian which means that the null space and range space of E are not compulsorily orthogonal spaces. The notation E represents an oblique projection which possessnull space and range space. An oblique projection can be adopted to disintegrate*x* into its constituents in two disjoint vector spaces that are not limited to be orthogonal. Two subspaces are said to be disconnected if the only connecting vector is the zero vector [8]. Oblique projections are adopted around the QSP framework to create new frames classes, a general sampling framework and effective subspace detectors for reconstruction and sampling in arbitrary spaces.

3.0 APPLICATION OF QUANTUM SIGNAL PROCESSING IN STRENGTHENING CYBER DEFENSE

Currently, the online security space has been on rampage due to the improving number of cyber-attacks being experienced globally on daily basis. The companies are developing essential security framework in their different set-up. However the process becomes discouraging and impracticable for executive digital computers. Therefore, cybersecurity has a vital subject of discussion around the world. The increase in the over-reliance on digitalization has greatly influenced its vulnerability to threats. Quantum computing with the aid of machine learning can assist in the development of different techniques to tackle these cybersecurity attacks [16].

Quantum signal processing techniques are essential area in security world due to the possible digital information vulnerability to attack and its connection with other techniques. It is an established fact that quantum technologies will certainly bring a remarkable strategic purpose. This will also delivereconomic and politicalbenefits. At the heart of this is the influence of quantum computing in cryptography. Huge amounts and extremely significant data can be approached with these technologies. This deliverssubstantial threat to existing technological infrastructure. In order to secure communication systems and data from these attacks, the Cryptography is adopted. Cryptography is a vital area in which quantum computing has instant effects on cyber security. Public key encryption is broadly adopted in the encryption of almost all importantdata transferred and communications on the internet and the cloud. Every internet browser which is presently adopted has the important public - key encryption assembled to safeguard traffic over the disclosed internet [17].

Many businesses usually adopt public key encryption to defend their communications, internal data and user access to connected devices. Cyber security influences computer systems security from interruptions that might damage the software, data or hardware. The permission of illegal usage increase the exposing risk of private information causing damage or interruption. The quantum encryption is usually adopted to protect the CPS's classical communications infrastructure that are difficult to be disengaged by quantum computers. The shift to remote work and the improving digitalization have caused the increase in the number of cyberattacks. Entities which store sensitive data after collecting them such as intellectual property irrespective of size or sector are at a greater risk of being chosen for a cyberattack like sabotage or espionage [18].

For instance, the theoretical conjectures scenario about RSA-2048 bit decryption possessing quantum accelerators can be considered. Recently, Google evaluate 20 million NISQ device qubits to disrupt an RSA key within the period of 8h. Simultaneously, the latest improvements in physical qubits have not authoritativelygo beyond the 100 qubit mark for NISQ devices, without digital annealer techniques. In this case, special applicable analog optimization machines are used. Other theoretical improvementshave the possibility of disintegrate RSA-2048 encryption having 13436 qubits within the period of 177 Days. Also, the multimode quantum memory principle which is still the same as theoretical presumption has not been detected. Even though there is existence of a quadratic speedup as a result of a Grover algorithm designed for quantum accelerated pre-sampling to basic force key search against AES, the breakage of anything above AES-256 bitkey length together with supercomputers is not possible [15]. Based on this, there was a serious argument among researchers that classified and encrypted data havingshorter key length than AES-256 and longer intelligence life, can be broken after storing in the future. These may experience quantum attack from the future. However, intelligence having a shorter lifetime is not influencedconsidering the fact that decryption might take months. Thus, the quantum computing devices reverse threatis far and the data intelligence life are very important.

3.1 DEFENSIVE CYBER SECURITY MEASURES AND MITIGATIONS

The first step in cyber security defense is identifying your personal technology environment and stack. Systems that possess great cybersecurity maturity level show security operation programs having extensive monitoring and logging for response activities and detection of threat. Based on the application, processes or system, there is often a trade-off between available resources and cost. The identification of significant risks to your critical processes and assetsfacilitates in putting vigorous security controls into places. People awareness and cyber hygiene should be the first line of defense one can simply strengthen [19].

The distant work policies should be put in place as the attack surface enlarges intoemployees homes' and cloud. This implies that there is need for endpoints to be secured, data in transit and at rest should be encrypted. With reference to critical assets and applications; and the risk appetite, cloud and hybrid architectures are required need to be adequately configured regarding authorization, segmentation, encryption and authentication for significant perimeters with DMZs (Demilitarized Zone in perimeter networks) and firewalls or follow a complete zero trust model if it is allowed by resources [20]. Security reviews and cloud security gap analyses assist in searching forweaknesses and misconfigurations. Non-production environments are advised not to be ignored particularly research and development systems. With reference to legacy software, for example in ICS systems, migration of OPC classic to OPC UA should be executed and further segmented to close the threat aperture with DMZs,instantiate firewalls and AAA (Authentication, Authorization and Accounting), where it is functional. Quantum Computing Systems admire a mixture ofproprietary hardware and software with off-the shelf components. This exhibits the responsibility for flashing by design and discharging source-code bug fixes if it is for commercial purpose. The responsibility in off-the shelf components falls with the recognition of vulnerabilities and strengthening them [18].

Taking a deep consideration of control systems, segmentation of the fail-safe systems should be done in order to prevent single-points of failure. For example, there should not be accessibility of control unit and cooling system of the ADI/QPU by an attacker via the same Host-CPU for a disruption threat on a compromised Quantum Computing System. In ICS environments, the people vector is also essential.

An air-gapped system can only be penetrated by connecting that space to gain physical access. Unlawful access by an unaware employee or insider threatcan be controlled by closely locking up physical access, only whitelisting permitted USB sticks and/or having a device antivirus scan stage executed [21].

4.0 CONCLUSION

This manuscript has examined the concepts of Quantum Signal Processing and cyber defense. The measurement consistency principle, quantization of the measurement output principle and measurement concept were the three interconnected fundamental principles of quantum mechanics that are very active in Quantum Signal Processing. Quantum physics relationship to QSP framework and relevant key results was also examined. The design of algorithm in the quantum signal processing framework was also discussed with major considerations given to modification of known algorithms, measurement parameters utilization, probabilistic mappings, imposition of inner product constraints and oblique projections. Lastly, application of quantum signal processing in strengthening cyber defense was also considered. Nonetheless, defensive cyber security measures and mitigations were also presented. In conclusion, Quantum Signal Processing is applicable in strengthening cyber defense.

REFERENCES

[1] Bindhu V. Cyber Security Analysis for Quantum Computing", Journal of IoT in Social, Mobile, Analytics, and Cloud, 2022; Volume 4, Issue 2, 133-142 133.

[2] Phillipson F, Wezeman RS, Chiscop I. Indoor–Outdoor Detection in Mobile Networks Using Quantum Machine Learning Approaches, Computers, 2021; 10, 71,

[3] Havlíček V, Córcoles AD, Temme K, Harrow AW, Kandala A, Chow JM. Supervised learning with quantum enhanced feature spaces, Nature. 2023; 567(7747):209-12.

[4] Shen J, Zhou T, Chen X, Li J, Susilo W. Anonymous and Traceable Group Data Sharing in Cloud Computing. IEEE Transactions on Information Forensics and Security. 2018; 13, 4, 912-925.

[5] Bartolucci S, Birchall P, Bomb´ın H, Cable H, Dawson C, Gimeno-Segovia M, Johnston E, Nickerson KKN, Pant M, Rudolph FPT, Sparrow C. Fusion-based quantum computation. Nature Communications. 2023; 14(1):912.

[6] Babbush R, McClean JR, Newman M, Gidney C, Boixo S, Neven H. Focus beyond quadratic speedups for error-corrected quantum advantage. PRX Quantum, 2021; 2(1), 27-39.

[7] Adhikary S, Dangwal S, Bhowmik D. Supervised learning with a quantum classifier using multi-level systems, Quantum Information Processing. 2023; 19(3):89.

[8] Hoefler T, Haner T, Troyer M. Disentangling hype from practicality: On realistically achieving quantum advantage. Communications of the ACM. 2023; 66(5):82–87.

[9] Maslov D, Jin-Sung K, Bravyi S, Yoder TJ, Sheldon S. Quantum advantage for computations with limited space. Nature Physics. 2021; 17(8):894–897.

[10] Satwik K, Swaroop G. Security Aspects of Quantum Machine Learning: Opportunities, Threats and Defenses" (Invited), arXiv:2204.03625v1 [cs.CR] 7 Apr 2022.

[11]. Abdullah AS, Mahabubul A, Swaroop G. Analysis of Crosstalk in NISQ Devices and Security Implications in Multi-Programming Regime", In Proceedings of the ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED '20), Association for Computing Machinery, 25–30, 2022

[12] Zlokapa A, Villalonga B, Boixo S, Lidar DA. Boundaries of quantum supremacy via random circuit sampling. npj Quantum Information. 2023; 9(1):36-49.

[13] Wu Y, Bao WS, Cao S, Chen F, Chen MC, Chen X, Chung TW, Deng H, Du Y, Fan D, Gong M. Strong quantum computational advantage using a superconducting quantum processor. Phys. Rev. Lett. 2021; 127, 180501.

[14] Arute F, Arya K, Babbush R, Bacon D, Bardin JC, Barends R, Biswas R, Boixo S, Brandao FGSL, Buell DA. Quantum supremacy using a programmable superconducting processor. Nature. 2019; 574, 7779, 505–510.

[15] Petros W, Elham K. Cyber security in the quantum era", Commun. ACM. 2019; 62, 4, 120. https://doi.org/10.1145/3241037.
[16] Ekert AK. Quantum cryptography based on bell's theorem. Phys. Rev. Lett. 1991; 67, 661–663.
[17] Yadav SP, Singh R, Yadav V, Al-Turjman F, Kumar SA. Quantum-Safe Cryptography Algorithms and Approaches: Impacts of Quantum Computing on Cybersecurity. 2023; Walter de Gruyter GmbH & Co KG.
[18] Rangan KK, Abou Halloun J, Oyama H, Cherney S, Assoumani IA, Jairazbhoy N, Ng SK Quantum computing and resilient design perspectives for cybersecurity of feedback systems. IFAC-Papers OnLine. 2022; 55(7), 703-708.
[19] Said D. Quantum Computing and Machine Learning for Cybersecurity: Distributed Denial of Service (DDoS) Attack Detection on Smart Micro-Grid. Energies. 2023; 16(8), 3572.
[20] Zago M, Gil P´erez M., Martinez Perez G. Early DGA-based botnet identification: Pushing detection to the edges, Cluster Comput, 2021. DOI: 10.1007/s10586-020-03213-z.
[21]. Singh, M., Singh, M. and Kaur, S. Issues and challenges in DNS based botnet detection: A survey", Computers & Security, 2019; Vol.86, pp.28–52, DOI: 10.1016/j.cose.2019.05.019.