Cyber Security Risks and Mitigation Related to Quantum States and measurement challenges

A.Johnbasco Vijay Anand, Dr. S. Sukumaran

Ph.D. Research Scholar, Department of Computer Science, Erode Arts and Science College, Erode 638009, TN, India,

Associate Professor of Computer Science, Erode Arts and Science College, Erode 638009, TN, India

Abstract— **Thought Quantum computers bring in transformative leap forward in computational capabilities, offering unprecedented potential for advancements[1] in cybersecurity, it also introduces new and potent threats that must be addressed. This research article underscores the improvements in cybersecurity that quantum computing has ushered in, while acknowledging the imperative need for comprehensive threat modeling[2] to anticipate and mitigate quantum threats. This research article explores threat modeling and risk assessment while leveraging real-time quantum computers across various aspects, including maintaining entangled states, achieving high-fidelity gate operations[5], error correction techniques, quantum measurements, qubit stability, coherence preservation[3], quantum decoherence, quantum noise and superposition/entanglement in quantum sensing and measurement devices. For each aspect, we identify threats, perform threat modeling and discuss cyber security risks and mitigation strategies to enable the secure integration of quantum computing technologies.**

Index Terms **—Quantum security; Quantum Threats; Quantum Threat Modeling; Quantum Risks.**

I. INTRODUCTION

The integration of real-time quantum computers into various domains presents both immense opportunities and significant security concerns. This research article embarks on a journey through the intricate landscape of quantum computing, shedding light on the advancements it has brought to the realm of cybersecurity, while also delving into the critical need for threat modeling and risk assessment. This article also explores several facets of quantum computing, each presenting unique opportunities and risks:

Maintaining Entangled States:
Quantum computers harness the power of entanglement, a phenomenon where quantum particles become correlated in such a way that the state of one particle depends on the state of another, regardless of the distance between them. Maintaining entangled states is crucial for quantum computation, but it is susceptible to environmental noise[4] and hardware failures. We will explore threat modeling for entanglement preservation and the mitigation strategies required to combat these threats.

Achieving High-Fidelity Gate Operations:
Quantum gates are the building blocks of quantum circuits and achieving high-fidelity gate operations is paramount for accurate computation. Control errors and crosstalk between qubits can lead to gate operation errors. This article will discuss threat modeling for gate fidelity and strategies to achieve precise gate operations.

Error Correction Codes and Techniques:
Error correction is pivotal in mitigating quantum errors. Quantum systems are inherently fragile and undetected errors [6]can lead to incorrect results. We will examine error correction codes and techniques, delving into their threat modeling and their role in ensuring the reliability of quantum computations.

Quantum Measurement Processes:
Quantum measurement is a fundamental aspect of quantum computing, but it is not immune to errors. Accurate measurements are essential for extracting meaningful information from quantum states. This section will explore the challenges of quantum measurement, threat modeling for measurement accuracy and strategies to enhance the precision of measurement processes.

Qubit Stability and Measurement:
Quantum bits (qubits) must be stable to maintain quantum coherence, which is essential for quantum

computation. Threats to qubit stability and measurement errors[7] can compromise results. We will delve into the world of qubit stability, threat modeling for stability preservation and verification techniques for precise measurement.

Preserving Coherence in Quantum Systems:

Quantum coherence lies at the heart of quantum computing. However, maintaining coherence over extended periods is a formidable challenge due to environmental factors and hardware instabilities. We will investigate the mathematical and physical aspects of coherence preservation[8] and the risk mitigation strategies that are indispensable.

Quantum Decoherence and Quantum Noise:

Quantum decoherence and noise are formidable adversaries in the quantum realm. Environmental noise and hardware imperfections can disrupt quantum states.

Superposition and Entanglement in Quantum Sensing and Measurement Devices:

Beyond computation, quantum properties like superposition and entanglement [9]find applications in quantum sensing and measurement devices. However, these devices are not immune to interference and inaccuracies. We will discuss the potential threats to quantum sensing and measurement devices and strategies to ensure the integrity of the measurements.

II. MAINTAINING ENTANGLED STATES

Threats: Environmental noise, Hardware failures:

Effective threat models should mandate the implementation of shielding and isolation techniques to counter environmental noise. They must demand rigorous identification and assessment of noise sources that could disrupt entangled states. Furthermore, they should insist on redundancy as a protective measure against hardware failures, accompanied by the incorporation of error correction codes[10] to rectify and fortify quantum states. Example: A threat model should specify the use of specialized shielding materials and isolation chambers to eliminate external electromagnetic interference that could compromise the entanglement of qubits in a quantum communication system. Additionally, the model should mandate the presence of backup qubits and real-time error correction algorithms to recover from hardware failures and maintain entanglement.

The entangled state can be represented by:

$$\rho = | \psi \rangle\langle\psi |$$

In this formula:

ρ represents the density matrix of the quantum system.

$| \psi \rangle$ is the ket notation for the entangled state.

Threat Modeling: Implement Noise-Resistant Shielding and Isolation, Require Redundancy and Quantum Error Correction[10]

To combat environmental noise, threat models should specify the implementation of noise-resistant shielding materials, such as superconducting materials and Faraday cages, coupled with stringent isolation measures. Threat models must explicitly require the identification and evaluation of noise sources, insisting on noise-tolerant quantum hardware. Additionally, models should mandate redundancy through the use of backup qubits and real-time error correction codes, such as the surface code, to address hardware failures effectively.

Example: In a practical scenario, a threat model could demand the utilization of cryogenic shielding[11] and Faraday cages in a quantum computing laboratory to shield qubits from external electromagnetic interference. Furthermore, the model should require the presence of backup qubits and the continuous monitoring of error rates, with the stipulation that error correction algorithms must be automatically applied to ensure qubit stability and entanglement preservation.

Risks: Availability of Data on Entangled Qubits and Eavesdropping on entangled qubits.

The risk of unauthorized access and exposure of data related to entangled qubits poses a substantial threat to quantum entanglement systems. Threat models should prioritize mitigating this risk.

The risk of eavesdropping[26] on entangled qubits is not theoretical but a genuine concern in quantum communication[12]. Threat models must mandate rigorous security measures.

Mitigation: Enforce Quantum Key Distribution (QKD) for Unbreakable Security

Effective threat models should not merely suggest but insist on the incorporation of Quantum Key Distribution (QKD) as the primary mitigation strategy. They must unequivocally state that QKD is the gold standard for securing data on entangled qubits.

Example: Threat models should specify that all quantum communication protocols involving entangled qubits must utilize QKD, such as the BBM92 or E91 protocols. QKD guarantees that any interception or tampering attempt will be detected due to the fundamental principles of quantum mechanics, ensuring the absolute confidentiality and integrity of data on entangled qubits. These measures are essential, as demonstrated by real-world implementations of QKD in secure quantum networks and quantum cryptography applications.

In summary, practical threat models[13] must go beyond abstract descriptions and outline specific technological measures to address and mitigate risks. These measures, including noise-resistant shielding, redundancy, error correction and the strict enforcement of QKD protocols, are essential to enhance the security of quantum entanglement against real-world threats like environmental noise, hardware failures and the unauthorized availability of data on entangled qubits.

III. ACHIEVING HIGH FIDILITY GATE OPERATIONS

Threats: Control errors, Crosstalk:

In the pursuit of high-fidelity gate operations in quantum computing, we must address threats stemming from control errors and crosstalk. To ensure secure and precise quantum computation, threat models should proactively address these challenges.

Quantum Process Tomography approach helps assess the fidelity of quantum gate operations:

Threat Modeling: Mandate Error Correction and Fault-Tolerant Techniques, Insist on Qubit Isolation[14]

Effective threat models should not merely recognize but mandate the implementation of error correction and fault-tolerant techniques to counter control errors. These models must insist on rigorous testing and validation of control systems, ensuring their accuracy and reliability. Additionally, they should emphasize the importance of qubit isolation to minimize crosstalk[15] and unwanted interference.

Example: In a practical scenario, a threat model for high-fidelity gate operations could specify the utilization of established error correction codes such as the surface code or the repetition code. It should mandate continuous monitoring of control parameters and immediate correction of any deviations. Furthermore, the model should require the physical isolation of qubits, ensuring that crosstalk remains below specified tolerances.

Risk: Unauthorized Gate Manipulation

The risk of unauthorized manipulation of quantum gates presents a significant cybersecurity challenge in quantum computing. Threat models should focus on mitigating this risk by incorporating robust security measures.

Mitigation: Enforce Access Control and Cryptographic Protections

Effective threat models should insist on the implementation of access control mechanisms and cryptographic protections to safeguard quantum gates against unauthorized manipulation.

Example: Threat models should specify the use of access control policies that restrict gate manipulation to authorized personnel only. Moreover, cryptographic protections[15] should be enforced to ensure the integrity and authenticity of gate operations. These measures will prevent unauthorized entities from tampering with quantum gates, thereby preserving the security and reliability of quantum computations.

In summary, practical threat models must be proactive and prescriptive in addressing risks associated with achieving high-fidelity gate operations in quantum computing. By mandating error correction, fault-tolerant techniques, qubit isolation, access control and cryptographic protections, these models enhance the security of quantum gate operations while ensuring the precision and integrity of quantum computations.

IV. ERROR CORRECTION CODES AND TECHNIQUES

In the area of error correction in quantum computing, threats stemming from undetected errors and resource overhead pose significant challenges. It is imperative to address these threats effectively to ensure the reliability of quantum computations.

Correction can be achieved by:

$$S|\psi\rangle=|\psi\rangle$$

Where, S represents the stabilizer group of the quantum error correcting code and $|\psi\rangle$ is the quantum state encoded in the code.

Threat Modeling: Mandate Robust Error Correction Codes, Require Resource Optimization
Comprehensive threat models must go beyond acknowledging these threats and instead mandate the use of robust error correction codes capable of detecting and correcting errors effectively. Additionally, they should require resource optimization strategies to manage the computational overhead associated with error correction.
Example: In practice, a threat model for error correction should stipulate the use of powerful error correction codes, such as the surface code or the Steane code, which provide high-level error detection[16] and correction capabilities. It should also emphasize the development and implementation of resource-efficient algorithms to minimize computational demands.

Risk: Attack on Error Correction Mechanisms
The risk of malicious attacks targeting error correction mechanisms is a critical cybersecurity concern in quantum computing. Threat models should prioritize mitigating this risk through robust security measures.

Mitigation: Enforce Secure Error Correction Protocols
Effective threat models should insist on the implementation of secure error correction protocols that protect against attacks and ensure the integrity of error correction processes.
Example: Threat models should specify the use of cryptographic techniques, such as digital signatures or encryption, to secure error correction protocols. Additionally, they should mandate rigorous access controls to prevent unauthorized tampering with error correction mechanisms. These measures will safeguard error correction processes [17]against external threats and manipulation attempts.
In summary, practical threat models must be prescriptive in addressing risks associated with error correction in quantum computing. By mandating the use of robust error correction codes, resource optimization, secure error correction protocols and stringent access controls, these models enhance the security of error correction mechanisms while ensuring the accuracy and reliability of quantum computations.

V.QUANTUM MEASUREMENT PROCESS

Threats: Measurement Errors and Quantum Backaction
In the domain of quantum measurement processes, threats originating from measurement errors and quantum backaction demand careful consideration. These threats can significantly impact the accuracy and reliability of quantum measurements.
Measurement is achieved through the below formula:

$$P(\alpha_i)=|\langle\alpha_i|\psi\rangle|^2$$

Where: $P(\alpha_i)$ represents the probability of obtaining the eigenstate $|\alpha_i\rangle$ as a measurement outcome, $|\alpha_i\rangle$ are the eigenstates of the observable $A^\wedge$. (A Cap) and $|\psi\rangle$ is the initial quantum state

Threat Modeling: Mandate Calibration, Error Correction and Adaptive Measurement Strategies
Thorough threat models should not merely acknowledge these threats but should mandate specific actions to mitigate them effectively. These models must insist on the implementation of rigorous calibration[18] procedures to ensure the precision of quantum measurements. Additionally, they should require error correction mechanisms to rectify measurement errors in real-time. Furthermore, adaptive measurement strategies should be emphasized to adapt and optimize measurements dynamically.
Example: A practical threat model for quantum measurement processes[19] should outline precise steps for calibration, such as regular adjustments of measurement apparatus based on known standards. It should also mandate the integration of real-time error correction algorithms and the utilization of adaptive measurement techniques that respond dynamically to changing conditions.

Risk: Manipulation of Measurement Outcomes
The risk of malicious manipulation of quantum measurement outcomes poses a substantial cybersecurity challenge in quantum computing[19]. Threat models should prioritize mitigating this risk through robust security measures.
Mitigation: Enforce Quantum-Resistant Cryptographic Algorithms

Effective threat models should insist on the implementation of quantum-resistant cryptographic algorithms to secure measurement outcomes. These algorithms are designed to withstand attacks from quantum computers and ensure the integrity of measurement data.

Example: Threat models should specify the use of post-quantum cryptography, such as lattice-based cryptography or hash-based signatures, to protect quantum measurement data from tampering or manipulation. Implementing these algorithms ensures that measurement outcomes remain secure even in the presence of powerful quantum adversaries.

In summary, practical threat models must be prescriptive in addressing risks associated with quantum measurement processes. By mandating calibration, error correction, adaptive measurement strategies and the use of quantum-resistant cryptographic algorithms, these models enhance the security and reliability of quantum measurements while safeguarding against potential manipulation of measurement outcomes.

VI. QUBIT STABILITY AND MEASUREMENT

Threats: Qubit Decoherence and Measurement Device Errors

In the realm of qubit stability and measurement in quantum computing, two prominent threats emerge: qubit decoherence and measurement device errors. These threats can undermine the reliability and precision of quantum computations.

Threat Modeling: Mandate Active Qubit Control, Calibration and Verification

Effective threat models must do more than acknowledge these threats; they should mandate precise actions to mitigate them. These models must insist on active qubit control techniques to maintain qubit stability, preventing or mitigating the effects of decoherence. Additionally, they should require rigorous calibration and verification processes [20]to ensure the accuracy of measurement devices.

Example: A practical threat model for qubit stability and measurement should specify the use of techniques like quantum error correction and error-avoidance codes to actively control qubit parameters[21] and counteract decoherence. It should also mandate frequent calibration procedures for measurement devices, accompanied by rigorous verification steps to validate the accuracy of measurements.

Risk: Unauthorized Access to Qubit Parameters

The risk of unauthorized access to qubit parameters poses a critical cybersecurity concern in quantum computing. Threat models should prioritize mitigating this risk through stringent security measures.

Mitigation: Enforce Access Control and Authentication Protocols

Effective threat models should insist on the implementation of access control and authentication protocols to safeguard qubit parameters against unauthorized access.

Example: Threat models should specify the use of role-based access control (RBAC) mechanisms and strong authentication procedures to restrict access to qubit parameters. Implementing these measures ensures that only authorized personnel can modify or access critical qubit settings[21], protecting the integrity and security of quantum computations.

In summary, practical threat models must be prescriptive in addressing risks associated with qubit stability and measurement in quantum computing. By mandating active qubit control, calibration, verification, access control and authentication protocols[22], these models enhance the security and reliability of qubit operations while safeguarding against unauthorized access to qubit parameters. Pseudo code in Quantum specific language frm Microsoft (Q#), to measure the Qubit stability and accordingly apply error correction is as below:

```
operation MeasureQubitStability() : Result {
    mutable result = Zero;
    using (qubit = Qubit()) { // Allocate a qubit
        // Initialize the qubit
        Reset(qubit);

        // Apply quantum gates
        // (Example: H gate for putting qubit in superposition)
        H(qubit);

        // Measure the qubit
        set result = M(qubit);

        // Apply error correction if necessary
        // (Error correction logic goes here)
        // Reset the qubit
        Reset(qubit);
    }
    return result;
}
```

VII. PRESERVING COHERENCE

Threats: Environmental Factors and Hardware Instabilities

In the realm of preserving coherence in quantum systems, two pressing threats emerge: environmental factors and hardware instabilities. These threats can disrupt the delicate quantum states critical for quantum computation.

Threat Modeling: Mandate Temperature Control, Shielding and Hardware Parameter Monitoring

Effective threat models should not simply acknowledge these threats but prescribe concrete actions to mitigate them. These models must insist on precise temperature control measures to counteract the influence of environmental factors[17]. Furthermore, they should require shielding techniques to protect quantum systems from external interference. Additionally, threat models should emphasize continuous hardware parameter monitoring to detect and address any instabilities promptly.

Example: A practical threat model for preserving coherence in quantum systems should specify the use of cryogenic cooling [23]systems to maintain stable temperatures. It should also mandate the installation of shielding materials and Faraday cages to isolate quantum systems from external electromagnetic interference. Additionally, the model should require real-time monitoring of hardware parameters, with immediate corrective action in case of deviations.

Risk: Coherence Disruption Through External Interference

The risk of coherence disruption through external interference poses a significant cybersecurity concern in quantum computing. Threat models should prioritize mitigating this risk through robust security measures.

Mitigation: Enforce Quantum-Resistant Encryption for Data Protection

Effective threat models should insist on the implementation of quantum-resistant encryption algorithms to protect quantum data against unauthorized access and tampering.

Example: Threat models should specify the use of quantum-resistant encryption algorithms, such as lattice-based cryptography or code-based cryptography, to secure quantum data from potential threats. Implementing these encryption methods ensures the confidentiality and integrity of quantum data, even in the presence of powerful quantum adversaries.

In summary, practical threat models must be prescriptive in addressing risks associated with preserving coherence in quantum systems. By mandating temperature control, shielding, hardware parameter monitoring and quantum-resistant encryption, these models enhance the security and reliability of quantum systems while safeguarding against coherence disruption due to external interference.

VIII.QUANTUM DECOHERENCE AND NOISE

Threats: Environmental Noise and Quantum Hardware Imperfections

In the realm of quantum computing, two substantial threats demand attention: environmental noise and quantum hardware imperfections. These threats can lead to quantum decoherence and noise, risking the reliability of quantum computations.

$$d\rho/\, dt=--i/h[\mathcal{H},\rho]+\mathcal{L}(\rho)$$

Where: dp\dt represents the time derivative of the density matrix ρ, which describes the quantum state of the system.

$\mathcal{H}$ is the Hamiltonian operator representing the system's internal dynamics and $\mathcal{L}(\rho)$ represents the Lindbladian superoperator, which accounts for the effects of noise and decoherence on the quantum state.

Threat Modeling: Mandate Error Correction Codes, Shielding and Hardware Calibration

Effective threat models must move beyond acknowledging these threats and mandate concrete actions to mitigate them. These models should insist on the implementation of error correction codes to counteract the effects of quantum decoherence[19] and noise. Additionally, they should require shielding techniques to protect quantum hardware from environmental noise. Furthermore, threat models should emphasize regular hardware calibration to address imperfections and maintain the integrity of quantum hardware.

Example: A practical threat model for mitigating quantum decoherence[24] and noise should specify the use of advanced error correction codes, such as the surface code, to detect and correct errors in quantum computations. It should also mandate the installation of shielding materials and Faraday cages to minimize the impact of environmental noise on quantum hardware. Moreover, the model should require periodic hardware calibration to rectify imperfections and ensure quantum hardware's robustness.

Risks: Quantum Hardware Vulnerabilities

The risk of quantum hardware vulnerabilities poses a significant cybersecurity concern in quantum computing. Threat models should prioritize mitigating this risk through proactive security measures.

Mitigation: Enforce Continuous Monitoring and Patch Management

Effective threat models should insist on continuous monitoring of quantum hardware and the prompt application of patches and updates to address vulnerabilities.

Example: Threat models should specify the implementation of continuous monitoring systems that actively scan quantum hardware for vulnerabilities and anomalous behavior. Additionally, they should require a well-defined patch management process to ensure that any identified vulnerabilities are addressed promptly through updates or patches.

In summary, practical threat models must be prescriptive in addressing risks associated with quantum decoherence and quantum noise. By mandating error correction codes, shielding, hardware calibration, continuous monitoring and patch management, these models enhance the security and reliability of quantum computing systems while safeguarding against quantum hardware vulnerabilities.

IX. SUPERPOSITION AND ENTANGLEMENT IN QUANTUM SENSING AND MEASUREMENT DEVICES

Threats: Interference and Sensing Inaccuracies

In the realm of quantum sensing and measurement devices, two prominent threats emerge: interference and sensing inaccuracies. These threats can compromise the accuracy and reliability of quantum measurements.

Threat Modeling: Mandate Shielding and Isolation Techniques, Require Calibration Procedures

Effective threat models should go beyond acknowledging these threats and prescribe precise actions to mitigate them. These models must insist on the implementation of shielding and isolation techniques to protect quantum sensing[18] and measurement devices from interference. Furthermore, they should require rigorous calibration procedures to ensure the accuracy of measurements.

Example: A practical threat model for quantum sensing and measurement devices should specify the use of specialized shielding materials and Faraday cages to minimize external electromagnetic interference. It should also mandate frequent calibration procedures to verify and adjust the accuracy of measurement devices.

Risk: Manipulation of Sensing Data

The risk of malicious manipulation of quantum sensing data poses a significant cybersecurity concern. Threat models should prioritize mitigating this risk through robust security measures.

Mitigation: Enforce Cryptographic Integrity Checks

Effective threat models should insist on the implementation of cryptographic integrity checks to protect sensing data from unauthorized manipulation.

Example: Threat models should specify the use of cryptographic techniques, such as digital signatures or message authentication codes (MACs), to ensure the integrity of sensing data. Implementing these measures guarantees that any unauthorized manipulation or tampering with the data will be detected, preserving the accuracy and reliability of quantum sensing[18] and measurement outcomes.

In summary, practical threat models must be prescriptive in addressing risks associated with superposition and entanglement in quantum sensing and measurement devices. By mandating shielding, isolation techniques, calibration procedures and cryptographic integrity checks, these models enhance the security and reliability of quantum sensing and measurement systems while safeguarding against data manipulation threats.

V. CONCLUSION

This research article has provided an in-depth analysis of threat modeling and risk assessment while leveraging real-time quantum computers. While Quantum Computers may elevate Confidentiality and Integrity of the data in transit and data at store, threats may mainly emerge from the adversaries who wanted to target Availability in the CIA triage. By identifying threats, performing threat modeling and discussing cyber security risks and mitigation strategies[23] for various aspects of quantum computing, organizations and researchers can better prepare for the secure integration of quantum technologies into their systems and applications, ensuring the realization of quantum computing's potential while mitigating associated risks.

REFFERENCE

[1] Steane, A. M. (1997). "Active stabilization, quantum computation and quantum state synthesis." Physical Review Letters, 78(11), pp. 2252-2255.

[2] Preskill, J. (1998). "Reliable quantum computers." Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, 454(1969), pp. 385-410.

[3] Nielsen, M. A., & Chuang, I. L. (2000). "Quantum Computation and Quantum Information." Cambridge University Press.

[4] Shor, P. W. (1997). "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM Journal on Computing, 26(5), pp. 1484-1509.

[5] Aharonov, D., & Ben-Or, M. (2008). "Fault-tolerant quantum computation with constant error." SIAM Journal on Computing, 38(4), pp. 1207-1282.

[6] Lidar, D. A., & Brun, T. A. (2013). "Quantum error correction." Cambridge University Press.

[7] Cory, D. G., Price, M. D., & Havel, T. F. (1997). "NMR techniques in the study of quantum computing." Progress in Nuclear Magnetic Resonance Spectroscopy, 32(4), pp. 115-129.

[8] Gottesman, D. (1997). "Stabilizer codes and quantum error correction." Caltech Ph.D. thesis.

[9] Preskill, J. (2018). "Quantum computing in the NISQ era and beyond." Quantum, 2, p. 79.

[10] Bouwmeester, D., Pan, J. W., Mattle, K., Eibl, M., Weinfurter, H., & Zeilinger, A. (1997). "Experimental quantum teleportation." Nature, 390(6660), pp. 575-579.

[11] Riebe, M., Häffner, H., Roos, C. F., Hänsel, W., Benhelm, J., Lancaster, G. P., ... & Blatt, R. (2004). "Deterministic quantum teleportation with atoms." Nature, 429(6993), pp. 734-737.

[12] Steane, A. M. (1996). "Multiple-Particle Interference and Quantum Error Correction." Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences, 452(1954), pp. 2551-2577.

[13] Gottesman, D. (1997). "Stabilizer codes and quantum error correction." arXiv preprint quant-ph/9705052.

[14] Giovannetti, V., Lloyd, S., & Maccone, L. (2004). "Quantum-enhanced measurements: Beating the standard quantum limit." Science, 306(5700), pp. 1330-1336.

[15] Caves, C. M. (1981). "Quantum-mechanical noise in an interferometer." Physical Review D, 23(8), pp. 1693-1708.

[16] Blais, A., Huang, R. S., Wallraff, A., Girvin, S. M., & Schoelkopf, R. J. (2004). "Cavity quantum electrodynamics for superconducting electrical circuits: An architecture for quantum computation." Physical Review A, 69(6), 062320.

[17] Wallraff, A., Schuster, D. I., Blais, A., Frunzio, L., Huang, R. S., Majer, J., ... & Schoelkopf, R. J. (2004). "Strong coupling of a single photon to a superconducting qubit using circuit quantum electrodynamics." Nature, 431(7005), pp. 162-167.

[18] Degen, C. L., Reinhard, F., & Cappellaro, P. (2017). "Quantum sensing." Reviews of Modern Physics, 89(3), 035002.

[19] Giovannetti, V., & Santamato, E. (2004). "Deterministic decoherence suppression for quantum systems." Physical Review A, 70(5), 052105.

[20] Zurek, W. H. (2003). "Decoherence, einselection and the quantum origins of the classical." Reviews of Modern Physics, 75(3), pp. 715-775.

[21] Breuer, H. P., & Petruccione, F. (2002). "The theory of open quantum systems." Oxford University Press. ISBN: 978-0199213900.

[22] Mosca, M., & Ekert, A. (2017). "The Market for Uncrackable Quantum Encryption is Here. Almost." Nature, 549(7672), pp. 188-189.

[23] Gheorghiu, A., Wallden, P., & Kashefi, E. (2019). "Efficient Verifiable Quantum Delegated Computation." Proceedings of the Royal Society A, 475(2220), 20190339.

[24] Bernstein, D. J. (2017). "Post-Quantum Cryptography." Nature, 549(7671), pp. 188.

[25] Karimipour, V. (2019). "Quantum Computing and Cybersecurity: Challenges Ahead." Proceedings of the Royal Society A, 475(2220), 20190243.

[26] Mosca, M., & Ekert, A. (2017). "The dangers of key reuse: Practical attacks on IPsec IKE." Proceedings of the

International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), pp. 201-216.

[24] Bernstein, D. J. (2009). "Grover vs. McEliece." Advances in Cryptology – EUROCRYPT 2009, pp. 73-90.

[25] Svore, K. M., Geller, A., Troyer, M., Azariah, J., Granade, C., Heim, B., Kliuchnikov, V., Mykhailova, M., Paz, A., & Roetteler, M. (2018). "Q#: Enabling Scalable Quantum Computing and Development with a High-level DSL." Proceedings of the Real World Domain Specific Languages Workshop 2018, pp. 7:1–7:10.

AUTHOR PROFILE

Dr. S. Sukumaran, working as Associate Professor, Department of Computer science (Aided) in Erode Arts and Science College, Erode, Tamil Nādu, India. He is a member of Board of studies in various Autonomous colleges and universities. In his 35 years of teaching experience, he has supervised more than 55 M.Phil. research works, guided 21 Ph.D. research works and still continuing. He has presented, published around 80 research papers in National, International Conferences and Journals. His area of research interest includes Digital Image Processing, Networking and Data mining.

Johnbasco Vijay Anand is a Ph.D. scholar (part time), Department of Computer science in Erode Arts and Science College, Erode, tamandu, India. He received his Master degree in Computer Application in 2001 from Bharathiar University. He is interested in advanced research in cyber security hardening techniques and methodologies using Quantum Computing and Artificial Intelligence.