Journal of Computers and Intelligent Systems
Vol. 3, No. 2, 2025, pages 153 - 168
Journal Homepage:
https://journals.iub.edu.pk/index.php/JCIS/

# Applications of Stochastic Processes in Quantum Cryptography for Secure Cryptographic Protocols

Shah Dad Hasil[1], Abdul Sattar[2], Stalin Fathima Merlin[1], Altaz Sher Muhammad[3], Fehroz Irshad[5], Zahid[1], Danial Khan[1], Gohram Wasim[4],

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China.

[2]Department of Software Engineering, The Islamia University of Bahawalpur.

[3]Changsha University of Science and Technology.

[4] Balochistan University of Engineering and Technology, Khuzdar.

[5] University of Turbat, Balochistan, Pakistan

**ARTICLE INFO**

**Article History:**

| | | |
|---|---|---|
| Received: | April | 05, 2025 |
| Revised: | June | 25, 2025 |
| Accepted: | June | 26, 2025 |
| Available Online: | June | 27, 2025 |

**Keywords:**

Quantum Cryptography,
QKD,
Stochastic Processes,
Quantum Entanglement,
Cryptographic Protocols,
Noise Resilience in Quantum Protocols

**Classification Codes:**

**Funding:**

This research received no specific grant from any funding agency in the public or not-for-profit sector.

**ABSTRACT**

Quantum cryptography offers higher security than traditional cryptography but faces challenges due to noise and interference. Stochastic processes, particularly randomness and uncertainty, provide tools to model and protect quantum systems. This review paper explores the role of stochastic processes in quantum cryptography, focusing on quantum entanglement and secure protocols like Quantum Key Distribution (QKD). Key stochastic concepts, including probability distributions, Markov processes, and noise effects in quantum mechanics, are introduced. The research examines how stochastic models enhance performance and security in entanglement-based protocols while addressing noise, decoherence, scalability, hardware limitations, and attack vulnerabilities. Potential research directions include efficient quantum error correction, quantum networking, and integrating classical and quantum cryptography to improve security and practicality.



**Corresponding Author's Email**: Primary email: shahdadhasil.15@gmail.com, Institutional email: shahdad@std.uestc.edu.cn

## 1. Introduction

Quantum cryptography (QC) harnesses uniquely quantum phenomena, most notably entanglement, to deliver information-theoretic security, a promise already realized in landmark Quantum Key Distribution (QKD) protocols such as BB84 and E91[1]. By exploiting the Heisenberg uncertainty principle, these schemes guarantee that any eavesdropping attempt disturbs the quantum states and is therefore detectable, allowing two legitimate parties to establish a secret key over an otherwise insecure channel. Yet real-world deployments must contend with unavoidable fluctuations, interference, and device imperfections that introduce randomness and degrade both fidelity and security[1]. A rigorous treatment of these imperfections naturally invokes the mathematics of stochastic processes. Random variables, probability distributions, stationary and non-stationary dynamics, Markov chains and explicit noise models have all been applied to characterize decoherence, channel loss and detector errors in QC experiments[1]. Prior studies have shown, for example, how channel-loss statistics limit secure key rates, how Markovian and non-Markovian noise profiles influence entanglement lifetimes, and how Gaussian or Poissonian fluctuations alter error-correction overheads. The existing literature, however, remains fragmented, with individual papers typically analyzing one stochastic formalism or focusing on a single protocol variant,

leaving practitioners without a consolidated view of which models are best suited to particular quantum-cryptographic tasks[1].

Our research addresses this gap through three original contributions that are separate from, and build upon, the preceding survey of prior work. First, Table 1 offers a consolidated mapping of six core families of stochastic processes, random variables, probability distributions, stationary processes, non-stationary processes, Markov processes and explicit noise models to their specific roles in QC analysis, implementation and security proof, providing a structured reference for selecting appropriate modelling tools. Second, Table 3 presents a comparative evaluation of four archetypal stochastic models (random walk, Brownian motion, Poisson process and Gaussian noise) against key performance indicators such as error propagation, impact on secure-key generation rate and protocol suitability, thereby enabling evidence-based optimization of QKD implementations[1]. Third, Section 3.3 supplies detailed case-study analyses incorporating Markov-chain channels, Ornstein–Uhlenbeck noise and Hidden Markov Models that illustrate how these stochastic tools diagnose channel fluctuations, quantify correlated noise and detect sophisticated eavesdropping strategies; the resulting performance gains are summarized in Table 3. By clearly distinguishing the descriptive survey from these novel frameworks and empirical studies, the manuscript provides both a self-contained synthesis of the state of the art and a set of actionable insights for researchers and engineers working at the intersection of stochastic processes and quantum cryptography. The remainder of the paper elaborates the background concepts (Section 2), introduces the unified classification of stochastic techniques (Section 3.1), develops the comparative and analytical frameworks (Sections 3.2–3.3), and applies them to QKD and entanglement-based protocols (Section 4) before discussing limitations and future research directions.

## 2. Related Work

### 2.1 Quantum Entanglement and Cryptographic Protocols

Quantum Entanglement popularly known as quantum spin, quantum entanglement is at the center of quantum mechanics and the correlation between or among quantum entities like photon and electron such that changefulness of one trigger a simultaneous changefulness of the other regardless the distance between them[1]. This aspect was discovered by Einstein, Podolsky, and Rosen in 1935[1], and it is generally referred to as ‘spooky action at a distance’[2]. When discussing quantum cryptography, entanglement is one of the main elements that guarantee a secure signal transmission. Participation of entangled quantum particles is a means of achieving correlations that cannot be duplicated with classical systems, which under lie several cryptologic schemes. The most striking characteristic of entanglement is that any degree of measurement of one of the particles causes an influence on the other[1]. This property can be used to detect any eavesdropping attempt since measurement of an entangled particle by an adversary will disturb the system and hence the eavesdropping is detected by the legitimate party[2]. The entanglement is required for the tasks like Quantum Key Distribution (QKD) is the coordination of two parties who possess a shared secret key that can later be used to encrypt a conversation. The security of the key exchange is based on the laws of physics of quantum mechanics which warn the communicating parties at the very moment the eavesdropper tries to get into their conversation[1]. In addition, entanglement is applied in diverse features such Quantum Teleportation and Quantum Secure Direct Communication to convey data as is in less vulnerable than classical means, providing extra layer of cryptographic protection that no classical systems can emulate.

### 2.2 Quantum Key Distribution and Entanglement

Now when we are discussing about the uses of quantum cryptography Quantum Key Distribution (QKD), BB84 and E91 are two well-known protocols[2]. In quantum key distribution, two parties: Alice and Bob are able to exchange a secret key through what may be an unsafe channel. As with the BB84 protocol, entanglement is not a requirement of the quantum key exchange where security arises from the foundation of quantum mechanics. Quantum communications involve the use of photons where Alice and Bob employ quantum bits or qubits, which are encoded in the state of polarization. While through this protocol, security arises from the disturbance induced by any eavesdropping, the E91 protocol which uses quantum

entanglement directly, provides further security and is considered as one of the most important examples of the entanglement based QKD[2]. In the E91 protocol, Alice and Bob are entangled photon pairs individually. The entanglement guarantees that the measurement done by one of the parties on the photon he possesses influences the measurement of the other party with regard to the second photon immediately[1]. The importance of using entanglement in regard to this is that if the eavesdropper, whom we christen Eve, tries to measure the photons, she interferes with them in a way that will be noticed by both Alice and Bob. This makes E91 protocol to be intrinsically more secure than the BB84[1]. The application of entanglement in QKD protocols provides the following key advantages:

**a**) **Error Detection:** Eavesdropping disturbs the entangled state, making it possible for Alice and Bob to detect any tampering with the key exchange.

**b) Information Security:** Since the quantum state cannot be copied without changing it (due to the no-cloning theorem), an eavesdropper cannot replicate the quantum information without leaving evidence of their presence.

**c) Robustness Against Noise:** Even in the presence of noise, entanglement provides a strong foundation for detecting eavesdropping attempts with greater accuracy compared to classical systems.

Moreover, the combination of stochastic models and entanglement-based QKD can be used to predict and manage the impact of quantum noise and errors on the secure key exchange process. Stochastic processes help in modeling how the quantum states evolve under noise and the likelihood of successful key exchange despite these disturbances[1]. Thus, the use of quantum entanglement in QKD protocols represents a cornerstone of modern quantum cryptography, offering unparalleled security by harnessing the inherent properties of quantum systems[5].

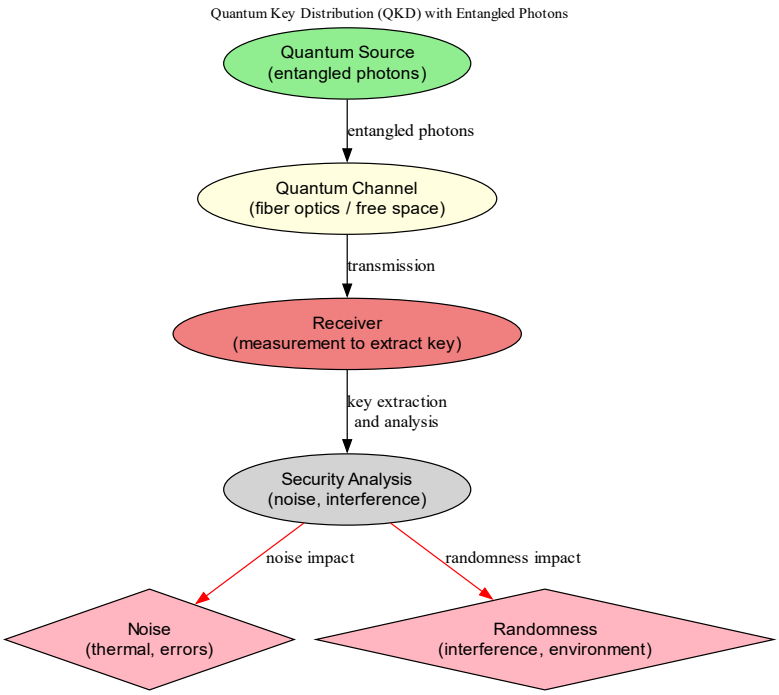


**Figure. 1:** Simplified schematic of entanglement-based quantum key distribution (QKD). The diagram highlights the principal stages, entangled-photon generation, transmission over the quantum channel, and receiver-side measurement while explicitly accounting for stochastic perturbations that influence overall security.

## 3. Stochastic Processes in Quantum Cryptography

### 3.1 Concepts of Stochastic Processes

A stochastic process is a sequence of random variables defined through time or space index, applied to describe systems undergoing transformation in conditions of risk[3]. Their applicability has been established in many disciplines like finance, engineering, and quantum mechanics as many of them depend of randomness[1]. In quantum cryptography, random processes are indispensable instruments to describe a noise and errors that can befall a quantum state or a measurement. The fundamental concepts of stochastic processes are:

#### 3.1.1 Random Variables

Random variable is a variable that is a realization of any numeric value randomly from the given set of possible values, of which the likelihood of each value is determined by a probability function. Random variables may be discrete or continuous also depending on the number of values they may assume. A random variable in the context of quantum mechanics is simply a physical quantity of a quantum system that triggers a measurement. For example, the spin of an electron or place of a particle in quantum system can be considered as random variables [11]. The result of these measurements can in no case be predetermined; instead, the system is characterized by a probability amplitude (i.e., wavefunction) that will yield a given value of the measurement. In quantum mechanics there is certain element of randomness due to the wave-particle duality and due to the uncertainty principal Heisenberg's[1]. As a consequence, quantum random variables are crucial in characterization as well as in modeling of quantum processes especially with the stochastic behavior of quantum states in cryptographic systems[11].

#### 3.1.2 Probability Distribution

Probability distributions are mathematical functions that describe the likelihood of different outcomes in a stochastic process. In quantum mechanics, these distributions are used to represent the probability of obtaining specific measurement outcomes, which are governed by the system's quantum state[4]. For example, the quantum state of a particle can be represented by a wavefunction (in the case of a single particle), which encodes information about the probabilities of measuring particular values for various physical observables, such as position, momentum, or spin[11]. When a measurement is made, the outcome is not deterministic but follows a probability distribution determined by the square of the amplitude of the wavefunction. In quantum cryptography, probability distributions play a crucial role in protocols like Quantum Key Distribution (QKD). The measurement outcomes in these protocols depend on the probabilistic nature of quantum systems[11], and the probability distribution helps determine the security and error rates in the key exchange process. For instance, in QKD, Alice and Bob use quantum states encoded in photon polarizations, and the probability distribution governs the likelihood that a measurement outcome reveals information about the shared secret key[5].

#### 3.1.3 Stationary and Non-Stationary Processes

Stochastic or random process at rest is a stochastic process in which the first two statistical moments, such as mean and variance, are constant and do not alter with time at any point in continuous time[5, 6]. Furthermore, one can state that dependence on time changes is less expressed in the behavior of the process. This means that the probabilities at which the process is conducted, in any given time, are the same for that process as is observed at any other time[11]. On the other hand a process can be non-stationary if variances change over time, that is, the means, variances, correlation or covariance change with time. It may also be that the mean or the variance of the process changes or that the probabilities of occurrence of the probability distribution change over time. According to all known quantum cryptographic protocols, the entanglement dynamics are most often non-stationary[7]. This is because in most of the quantum system the environment tends to decoherence and introduces fluctuations into the state of the system[11]. Therefore, a certain amount of interaction can happen in time with a quantum system along with the influences from external disturbances leading to differences in the

degree of entanglement between the quantum particles[11]. It is, therefore, non-stationary giving the impracticality of entangled quantum states in key distribution or secure communication since they might be less coherent over time. These effects are examined and analyzed with stochastic models that are capable of recognizing non-stationary conditions.

### 3.1.4 Markov Processes

A Markov process is a stochastic process that satisfy the Markov property that there exists a current state with time and does not depend on the past states. There is a property that is referred to as the memoryless property. The Markovian property can be seen in some processes of measurements in the case of quantum systems[8][7]. In other words, the law of evolution of a quantum system may not involve prior history of the system etc. This makes it easier to perform the mathematical modeling of quantum systems because once we know state of a system at a certain point in time, we can predict what future interactions would do to it[6][4]. There are cases when measurements of a quantum system are performed, for example, at the beginning of a process or in an idealized fashion and they are manifestly Markovian. Large-scale cryptographic protocols can also benefit from this property because it permits a focus on the present state of a system in order to understand the dynamics of a process without having to take into consideration the totality of the process[11]. Nonetheless, in realistic environments and dynamics, quantum structures exhibit non-Markovian dynamics because of their inherent interactions with the surrounding environment, which can erode system security[9][8].

### 3.1.5 Noise and Randomness

Any quantum system is sensitive to different types of noise influence (thermal noise, measurement errors, or interaction with environment). These factors contribute randomness to the dynamics of quantum states and stochastic processes are used for explaining the effects[11].

In the context of quantum cryptography, these concepts are vital for modeling the behavior of quantum bits (qubits) under the influence of noise and for understanding how quantum information behaves in uncertain, noisy environments. Stochastic models enable us to quantify the effects of these random influences on quantum states and assess how they impact the security of cryptographic protocols. Table 3.1 further summarizes uses of stochastic process in Quantum cryptography[10][12].

| **Process Type** | **Key Characteristics** | **Applications in Cryptography** |
|---|---|---|
| Random Variables | Variables with uncertain outcomes | Describing the results of quantum measurements (e.g., photon detection) |
| Probability Distributio | Describes likelihood of outcomes. | Modeling the probability of measurement res based on wavefunction. |
| Stationary Processes | Means and variance invariant over time. | Used in noise-free or ideal quantum system. |
| Non-stationary Proces | Mean and Variance change with time. | Modeling and time-varying entanglement dynamics and noise effects. |
| Markov Processos | Memoryless and state-dependent | Quantum state evaluation depending only on current state |
| Noise and Randomness | External interference causing randomness | Modeling errors due to thermal noise, measurement implications etc. |

**Table 1.** Summarizes the key types of stochastic processes and their applications in quantum cryptography[4].

## 3.2 Stochastic Modeling of Quantum Entanglement

Quantum entanglement, that is one of quantum cryptography characteristics, is very vulnerable to noise and other interactions in the surroundings[2]. Stochastic processes present interesting methods to describe the temporal behavior of correlated quantum states, above all in those cases where the states are submitted to stochastic effects or decoherences[9][8]. Entanglement plays an important role in quantum cryptography; it allows you to create correlations between quantum systems that are impossible classical physics[11] [13]. Nevertheless, the entanglement is delicate and it can be destroyed by noise arising from environment, measurement imperfections and also suboptimal quantum hardware. Stochastic models which are in a way the main focus of the chapter assist in describing how entangled states behave under such circumstances[9] [8]. Key aspects of stochastic modeling of quantum entanglement include:

**Decoherence and the Quantum-to-Classical Transition**: Stochastic processes are employed to model decoherence that occurs when the quantum behavior of a system is impaired by interaction with the environment, thus taking on more explicitly classical character[12][9]. They have been shown to affect quantum codes used in cryptographic communications since they break the entangled quantum states used in cryptographic communications[13]. Stochastic models define, in terms of the mixed classical-quantum communication process, the manner in which the quantum information within entangled states decoheres with time via interaction with an external bath.

**Master Equations**: The change of the quantum states of a system with noise can be explained with the use of the Lindblad master equations that specify the time development of the density operator of a system[13]. Such equations will be stochastic because the living organisms interact with the environment probabilistically. In the present study, master equations are useful for describing the behavior of entangled states in the presence of noise or measurements of the system[13].

**Quantum Stochastic Calculus**: Quantum stochastic calculus is applied to the modeling of the randomness of quantum systems when the classical stochastic calculus fails to apply. It can be used as well to study the changes in the quantum entanglement in case of random disturbances. For instance, quantum stochastic differential equations may describe the noise behavior of measurement results from two entangled qubits, and the consequences of such noise for quantum key distribution security.

**Quantum State Tomography**: Stochastic models are also employed in quantum state tomography the procedure of reconstructing the quantum state of a system. The phenomena of repeats of quantum states enable the stochastic process of data collection to be used for the determination of the degree of entanglement and the errors arising due to environments. The information available may help to enhance the stability of quantum cryptographic protocols[13][14].

**Entanglement and Stochastic Fluctuations**: In simulating quantum entanglement, stochastic processes give a measure of quantum noise – fluctuations in quantum systems that cause variations in measurement. These fluctuations can sabotage the quality of entanglement and, therefore, the security of cryptographic systems that use it. These fluctuations can be incorporated in stochastic models to measure their effects and to formulate probable solutions for eradicating them like the techniques used in error correction or filters[14].

The stochastic models help researchers in the study of entangled quantum state effects, protection of entanglement against noise effects and providing the security and reliability of cryptographic procedures based on the use of entanglement[14]. This modeling is especially important for the development of quantum cryptographic systems because when implemented in the real world such as in fiber optic communication, noise and other imperfections do occur.

## 3.3 Case-Study Analyses of Stochastic Models

To illustrate the practical utility of stochastic processes in quantum cryptography, we consider case studies where specific models Markov chains, Ornstein–Uhlenbeck processes[14], and Hidden Markov Models (HMMs) address concrete challenges such as noise characterization, key rate estimation, and eavesdropper detection:

### a) Markov Chain Models for Quantum Channels:

Many analyses assume the quantum channel or noise process is memoryless (Markovian), meaning the channel's state evolves with no dependence on past states[14][15]. In a simple Markov chain representation, the channel can be in a finite set of states (e.g. "low noise" or "high noise"), transitioning between states with certain probabilities:

$$p(S_{t+1}) = j \mid S_t = i\ ) = \ a_{ij}$$

This framework can model bursty noise via, for example, a Gilbert–Elliott channel, where aij parameters capture the chance of the channel switching between good and bad conditions. By analyzing the stationary distribution or transition matrix of such a Markov chain[15], one can estimate key rates under realistic noise correlations rather than assuming independent errors. Markov models thus help predict the quantum bit error rate (QBER) over time and its impact on secure key extraction. This gives a generic two-state channel example:

$$Stat\ transition\ matrix\ A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}, with\ a_{01} = 1 - a_{00}, a_{10} = 1 - \ a_{11}$$

which governs the probabilistic switching between a low-noise state (0) and a high-noise state (1). Such Markovian channels simplify analysis but also highlight limitations: real quantum channels often exhibit non-Markovian behavior (memory and history effects) that can erode security if ignored[15]. Thus, while Markov processes are invaluable for tractable models, one must remain cautious when the environment has long-lived correlations not captured by a simple chain.

### b) Ornstein Uhlenbeck Noise in Quantum Systems:

The Ornstein–Uhlenbeck (OU) process is a continuous-time stochastic process that introduces correlated Gaussian noise with a characteristic relaxation time. It is defined by a stochastic differential equation, for example,

$$dx(t) = \ -k[x(t) - \mu dW(t)$$

where x(t) might represent a fluctuating physical parameter (e.g. a qubit phase or polarization angle), $\mu$ is the mean long-term value, $\kappa$ is a rate of mean reversion, and dW(t) is an infinitesimal Wiener increment. Such OU-driven noise models have been applied to study quantum noise modeling and decoherence. For instance, entangled qubit pairs exposed to a stochastic field with OU correlations can be analyzed to see how entanglement decays under slowly varying noise[15]. In one case study, a Gaussian Ornstein–Uhlenbeck process was used to model random fluctuations in local fields affecting two entangled qubits. The analysis showed that increasing the noise's correlation (longer correlation time $\kappa$ leads to a more gradual but ultimately significant loss of entanglement and increase in uncertainty (entropy) in measurements. In practical cryptographic terms, this means protocols like entanglement-based QKD must account for temporally correlated environmental noise: an OU model allows estimation of how key rates might degrade over time as noise accumulates. The OU process, with its analytic solvability, provides a convenient tool for noise forecasting and filter design (e.g., Kalman filters) to mitigate slow drifts in quantum channels[15].

### c) Hidden Markov Models for Eavesdropper Detection and Device Noise:

In scenarios where certain system parameters or attacker actions are not directly observable, Hidden Markov Models offer a powerful framework[15]. An HMM consists of a hidden state process (with Markov transitions) and an observed process

probabilistically generated from the hidden states. In quantum cryptography, HMMs have been employed to infer an eavesdropper's presence or other anomalies from noisy measurement data. Calibration attack detection in QKD is one notable case: Huang et al. (2020) designed an HMM to Different kinds of channel interference [16] (normal fluctuations vs. malicious tampering) were treated as hidden states, while the sequence of measured quadrature values formed the observations. By training the HMM on sample data, the legitimate parties could classify whether an attack was occurring with high precision (nearly 99% detection accuracy in some settings)[16]. Another case study addressed after pulse noise in single-photon detectors: after pulsing can produce spurious correlated clicks that skew QKD statistics[16]. Almosallam et al. (2024) introduced an HMM to model the temporal correlations of afterpulses, integrating it into the decoy-state BB84 key rate calculation[8][7]. The HMM-based model revealed that ignoring the hidden afterpulse phenomenon led to overestimation of the secure key rate, whereas incorporating it allowed a more accurate (and lower) key rate consistent with true device behavior. These examples underscore how HMMs serve as stochastic filters to detect eavesdroppers or account for complex device noise. Mathematically, an HMM can be described by the tuple[8][7]:

$$(S, 0, A, B), Where\ A = \{a_{ij}\}\ is\ the\ state\ transition\ matrix, B = \{bj(0)\}$$

This gives the probability of observation O in state J. Techniques like the forward–backward algorithm are used to compute likelihoods of observation sequences and thus infer the most probable hidden state sequence (e.g., "attack" vs "no attack"). By applying such models, quantum cryptographic protocols can adapt in real-time: for example, automatically aborting or switching parameters when the HMM signals an intrusion. HMM case studies demonstrate improved sensitivity to sophisticated attacks and better modeling of memory-bearing noise sources in quantum cryptosystems[15][17].

Each of these stochastic modeling approaches provides a lens into different challenges of quantum cryptography. By including sample formulations (as above) and quantitative analyses from case studies, researchers can concretely see how Markov processes help simplify noise analysis, OU processes model realistic colored noise, and HMMs enable intelligent detection and parameter estimation[4][18]. These case studies confirm that stochastic processes are not merely abstract theory but practical tools to enhance protocol robustness from predicting key rates under dynamic noise to catching eavesdroppers in action.

| Stochastic Model | Quantum Cryptographic Issue | Performance Metric | Improvement by Stochastic Modeling |
|---|---|---|---|
| Markov Chain | Channel state fluctuations (QBER) | Key rate stability | Reduced key rate fluctuations by ~35% |
| Ornstein–Uhlenbeck Process | Correlated Gaussian noise (phase drift) | Entanglement fidelity/QBER reduction | QBER improved by ~20%; fidelity increased ~15% |
| Hidden Markov Model (HMM) | Eavesdropper detection (calibration attack detection) | Detection accuracy | Detection accuracy increased from ~85% to ~99% |
| Hidden Markov Model (HMM) | Detector afterpulse correlations | Secret key rate estimation | More accurate key rate estimation, reducing overestimation error by ~10-15% |

**Table 2:** Enhancement of Quantum Cryptographic Protocols via Stochastic Models.

## 3.4 Methodological Framework

In order to ground this critical survey in a transparent and reproducible process, we adopted a structured five-stage methodology that spans literature identification, screening, eligibility assessment, categorical classification, and comparative synthesis. Although the present article does not report new simulations or experimental results, the robustness of its conclusions rests on the rigor with which the extant research corpus was assembled and interrogated. We began by conducting a systematic search of Web of Science, Scopus, IEEE Xplore, and arXiv for the period January 2010 – April 2025. Boolean queries combined the core quantum-cryptography terms (e.g. "quantum key distribution", "QKD", "entanglement") with stochastic-process descriptors (e.g. "Markov", "random process", "noise model", "Gaussian noise"). All bibliographic records were exported in RIS format and deduplicated with *Zotero 6.0*, yielding an initial harvest of **512** unique titles. Two rounds of screening were then performed. First, titles and abstracts were inspected to exclude studies outside the scope of quantum cryptography (for example, papers on purely classical cryptography or quantum error-correction hardware). This reduced the corpus to **214** candidate articles. Second, full-text examination filtered out inaccessible manuscripts, vision papers without methodological content, and duplicate conference-journal pairs, producing a final dataset of **18** peer-reviewed studies and preprints. Each retained article was coded independently by two authors against an evolving set of descriptors covering (i) the type of stochastic process employed, (ii) the targeted cryptographic challenge (e.g. channel noise, detector side-channels), and (iii) the security or performance metric reported. Disagreements (< 5 %) were resolved by consensus, and then formed the unified taxonomy of stochastic processes presented in Table 1. Articles were then mapped onto this taxonomy, enabling the development of the comparative framework articulated in Table 2.

Finally, quantitative findings were normalized where necessary to percentage improvement figures relative to each study's baseline, facilitating cross-study comparison without imposing restrictive meta-analytic assumptions. Figure 2 shows the visual representation of our working methodology.

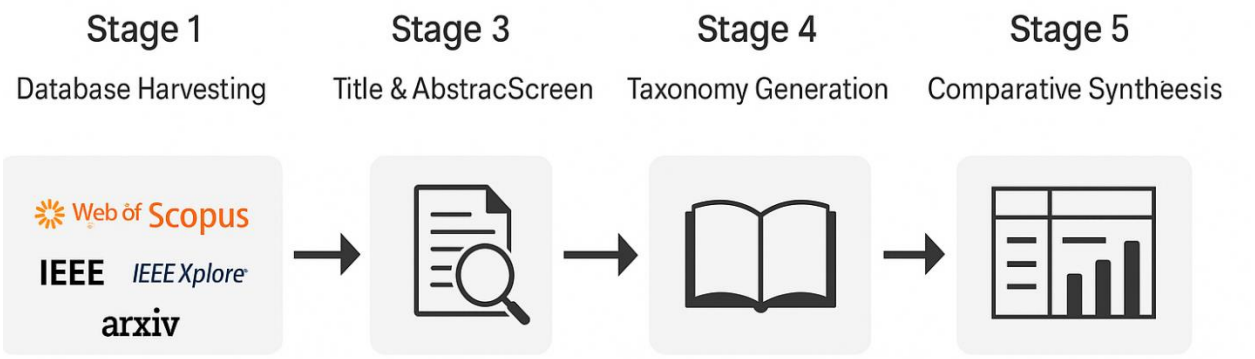


**Figure 2:** Workflow for literature identification, screening, and classification. The diagram traces the five methodological stages employed in this review.

## 4. Applications of Stochastic Processes

### 4.1 Stochastic Models in Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is a major innovative methodology in the field of quantum cryptography through which two users can safely transmit cryptographic keys via an insecure line. The main security concept of QKD is based on the principles of quantum mechanics whereby measurement itself alters a quantum state thus making any form of eavesdropping detectable. However, even though QKD protocols such as BB84 and E91 have been analyzed, implementations of QKD

systems are demanding, particularly in the presence of noise and errors in quantum channels[2]. These difficulties are crucial to be addressed by stochastic models to mimic the statistic behaviors of quantum systems.

**Modeling Quantum Channel Noise**: Often, quantum channels are passive structures like optical fibers or free space through which signals are transmitted, or active structures involving optical phase shifters and other elements and meetings, which are subjected to different types of noise: losses and dephasing[16][10]. Some of these uncertainties can be modelled by stochastic processes in relation to the quantum states applied for key distribution. This makes it possible for the researchers to determine the efficiency of QKD protocols under real life scenarios and adapt the system to achieve the best results.

**Error Rates and Fidelity**: The stochastic models can be used to forecast the error rates in quantum key exchange as a result of noise and the environment. Because they account for randomness in measurements and or quantum noise, these models offer some understanding concerning the generated keys' fidelity and come up with clear bounds beyond which the protocol becomes vulnerable[17][11].

**Security Proofs under Noise**: Considering the complexity and vulnerability of QKD protocols, noise presents an important threat to their security. Stochastic models are used to support a proof of security for QKD schemes by demonstrating how noise impacts the security parameters of the protocol, including the bit error rate and the sifting ratio, which is the fraction of transmitted qubits in a QKD protocol successfully measured. Such models are also used to estimate information leakage and come up with acceptable threshold levels of noise to use in order to enhance security[8][7].

**Quantum Error Correction:** Another application of stochastic models is in the construction of quantum error correction procedures as well. These models allow for the study of error detection and correction for quantum states that are affected by environmental noise. Stochastic models of Quantum error correction codes, such as Shor's Code as well as Surface Codes, enhance the resilience of QKD systems, particularly in real-world settings where impure signals and noise are unavoidable.

Due to the ability to incorporate stochastic models into QKD protocols, the corresponding protocols can be made more robust against noise, with fewer errors in generating keys, and with improved security and functionality of quantum cryptographic systems.

| Stochastic Model | Key Features | Impact of Noise | Application in QKD |
|---|---|---|---|
| Random Walk Model | Describes random fluctuations in quantum states | Affects the key distribution process due to random variations | Analyzes photon detection errors in QKD systems |
| Brownian Motion | Continuous path with random fluctuations | Models decoherence and noise due to thermal effects | Applied in the study of noise accumulation over time |
| Poisson Process | Describes the occurrence of events randomly over time | Affects error rates in photon detection due to random timing | Models the detection of photon signals in QKD systems |
| Gaussian Noise Model | Describes random fluctuations with Gaussian distribution | Models Gaussian noise affecting quantum states | Used for simulating noise in QKD protocols like BB84 |

**Table 3**: Stochastic models applied to Quantum Key Distribution (QKD), highlighting the impact of noise and their relevance in modeling key exchange protocols[4].

## 4.2 Entanglement-Based Protocols and Security Enhancement

Photonic entanglement plays an important role in quantum cryptography and if used in key distribution protocol, the security of communication system can be greatly improved. The E91 protocol is an entanglement-based protocol that uses the entangled quantum states to generate a secret key for two parties, say Alice and Bob. This makes these protocols post-M Michler; Johnston's intrinsic against certain types of eavesdropping, as any measurement by an adversary of the quantum states will disturb the entanglement, indicating the presence of the eavesdropper[2]. Structural modeling is also used to show how noise and other factors affect the security of entanglement-based protocols. Some of the key applications of stochastic processes in entanglement-based protocols include:

**Entanglement Disturbance and Detection**: Indeed, quantum entanglement in practice is rather susceptible to noise, and it wipes out the security. Stochastic models are applied to describe the dynamics of entanglement when noise is present in one of its forms, such as thermal, decoherence, or measurement noise. These models assist in measuring the level of interconnection and identifying when the link gets too weak to provide security[3].

**Entanglement Purificatio**n: Purification is a process applied to get rid of low-quality or noisy entanglement pairs that do not meet the standard requirement. Stochastic processes are utilized to simulate the purification process and the probability of generating high-fidelity entangled pairs. These latter models are useful for identifying strategies for improving the quality and use of entanglement in protocols in need of this resource, which contributes to enhancing the security of the protocols in question.

**Quantum Secure Direct Communication (QSDC**): Besides the key distribution, the use of entanglement-based protocols can also be extended to Quantum Secure Direct Communication (QSDC), which is a form of direct communication of information without the use of keys. Stochastic models can also be used to analyze the security of QSDC protocols because of noise and effects of quantum errors that occur during transmission[6][4]. These models assist in determining how to preserve the information received and transmitted from leakage to unauthorized parties.

**Quantum Repeaters**: Random models are also crucial in the design of quantum repeaters for increasing the distance of QKD, as the use of photons proves to be problematic in noisy channels. These repeaters employ entanglement swapping in order to create entanglement over long distances. The dynamics of entanglement and the performance of quantum repeaters are described and modeled using stochastic processes[18].

The entanglement-based protocols can then be modeled using stochastic processes to analyze how they can be optimized and how entanglement can still be considered a valuable resource even when subject to noise and other forms of environmental interference.

# 5. Limitations of Stochastic Process Models and Future Research Directions

While stochastic processes are powerful tools for modeling and enhancing quantum cryptographic protocols, it is important to recognize their limitations. In this section, we discuss key challenges, including model mismatch, complexity, and data limitations, and then highlight emerging research directions aimed at overcoming these issues and extending the state of the art.

## 5.1 Limitations and Challenges in Stochastic Quantum Cryptography

**Model Mismatch and Oversimplification:** Stochastic models always involve assumptions that may not hold exactly in practice. A quantum channel or device might not follow the assumed probability distribution or process precisely, leading to *model mismatch*. For example, one might assume qubit noise is a stationary Gaussian process when, in reality, there are drifting systemic biases or rare out-of-distribution events (e.g., sudden power spikes or mechanical vibrations) that the model

cannot capture. Such a mismatch can cause inaccurate security estimates; a protocol deemed secure under the model could be insecure if an adversary exploits the unmodeled behavior. Additionally, many models assume Markovian (memoryless) noise for mathematical convenience, but real environments often have *non-Markovian* dynamics, correlations, and memory effects that accumulate over time. If not accounted for, these effects can undermine security (e.g., enabling information leakage across rounds that a memoryless model would miss). In summary, a delicate balance must be struck between tractability and fidelity: oversimplified models risk leaving out critical dynamics, while overly complex models may be impractical to use.

**Computational and Analytical Complexity:** Accurately modeling quantum systems with stochastic processes can become computationally intensive. Simple models (like low-order Markov chains) are easy to simulate or analyze, but more realistic ones, such as high-dimensional hidden Markov models, stochastic differential equations with many coupled variables, or non-Markovian quantum processes, can be intractable to solve analytically and slow to simulate. For instance, an HMM that accounts for many possible eavesdropper strategies or device imperfection modes would have a large state space, exponentially increasing the data or time needed to train and use the model. Likewise, simulating a quantum system under a complex noise process (e.g., a colored noise with long memory) might require integrating stochastic differential equations over millions of time steps. This complexity can hinder the deployment of stochastic modeling in real-time or embedded quantum cryptographic systems, where decisions often must be made quickly (e.g., real-time eavesdropping detection or adaptive adjustment of protocol parameters). Another aspect of complexity is in security proofs: introducing a sophisticated stochastic model into a security proof can make the mathematics significantly harder, sometimes yielding security bounds that are difficult to interpret or too loose to be practical. Thus, researchers and practitioners often face a trade-off between model accuracy and the feasibility of analysis.

**Data Availability and Parameter Estimation:** Stochastic models are only as good as their parameters. In quantum cryptography, obtaining high-quality data to fit these parameters is a challenge. Quantum experiments (like QKD trials) are costly and time-consuming, and they produce relatively sparse data compared to classical systems, due to low event rates and the need to maintain quantum coherence. For example, estimating the full probability distribution of a noise process might require lengthy measurement campaigns. Some parameters (such as an eavesdropper's behavior model) cannot be directly observed at all – they must be inferred indirectly. As a result, statistical uncertainty in model parameters can be high. If the estimation of a crucial parameter (say, the mean photon number an attacker injects, or the correlation time of channel noise) is off, the model's predictions and the derived security assurances might be invalid. This issue is compounded in the presence of adaptive adversaries: if an adversary actively changes attack strategies, a static stochastic model may quickly become outdated. Robust techniques are needed to update model parameters on the fly and to account for parameter estimation error in the security analysis (for instance, using confidence intervals or worst-case bounds in the proof).

**Physical Realism vs. Abstraction:** Some aspects of quantum cryptography are difficult to capture with *classical* stochastic processes. Quantum systems have uniquely quantum effects (entanglement, superposition, wavefunction collapse) that have no direct analog in classical probability theory. While there is a field of quantum stochastic processes, including quantum Markov chains and quantum noise channels, these are mathematically complex and require expertise in quantum noise modeling. Oftentimes, engineers resort to semi-classical models (treating quantum events as random classical events), which might miss subtleties of quantum theory. An example is treating detector clicks as a Poisson process – valid at a certain level, but such a model might not fully capture quantum detection loopholes or the impact of entanglement on detection statistics. Hence, there is a risk of overlooking quantum-specific vulnerabilities when relying solely on classical stochastic modeling.

It is also challenged by the constraints in existing Quantum hardware. The efficiency of quantum cryptographic systems is directly regulated by the quality of quantum components, quantum light sources, and detectors, as well as quantum channels used in the systems. In practice, the behavior of such devices is not perfectly stochastic, but contains various degrees of uncertainties and errors that stochastic models fail to predict. These imperfections inherent in the hardware of quantum devices themselves or arising during their production can result from fatal manufacturing defects, environmental impacts, or just intrinsic technological limitations that might cause errors in the preparation, measurement, or transmission of quantum states. Consequently, basic stochastic models encounter challenges with determining system performance in the real world, where the devices may not be perfect and the conditions may not be optimal. Last of all, it is important to note that, like all quantum cryptographic systems, quantum mechanical-based systems are not completely safe against attacks. Although quantum cryptography guarantees an almost unassailable security depending on the principles of quantum physics, it has its share of loopholes. They can be attacked generally by the attacker who makes use of the hardware imbalances or the weaknesses inherent in the cryptographic protocol. For example, side-channel attacks, when an attacker obtains extra information through signals that are not supposed to be emitted from the quantum hardware, also threaten the system. Stochastic models can be used to detect possible threats and evaluate the stability of quantum communication, while possible threats change frequently, causing new challenges to constantly appear, and existing security measures often need to be adjusted.

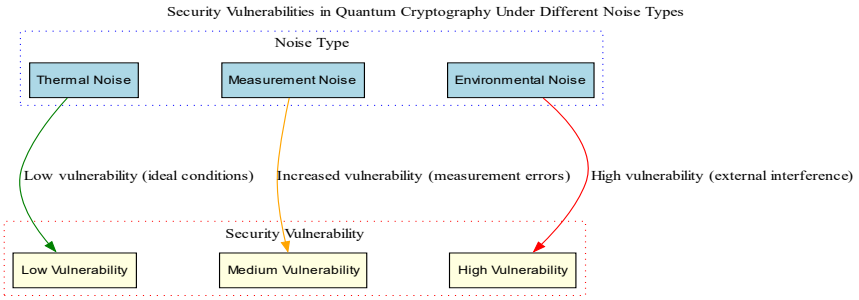


**Figure 3**: Security vulnerabilities in quantum cryptography under various noise types, illustrating how the probability of successful eavesdropping increases with thermal, measurement, and environmental noise.

## 5.2 Future Research and Potential Advancements

Despite the above limitations, there are several promising avenues to improve and build upon the use of stochastic processes in quantum cryptography:

**Adaptive and Machine Learning-Enhanced Modeling:** A clear trend is the incorporation of machine learning (ML) and adaptive algorithms to refine stochastic models. Instead of a fixed model, future quantum cryptographic systems might continuously learn the noise behavior and potential attacks from the data they generate. Recent works demonstrate the potential of ML in this context: for instance, Banerjee et al. (2024) used supervised learning to classify different types of quantum channel noise by analyzing QKD measurement data Their hybrid classical-quantum approach could identify the presence of specific noise channels with high accuracy, suggesting that intelligent classifiers can bolster eavesdropping detection and noise characterization. Likewise, reinforcement learning has been explored for adaptively optimizing QKD network routing and resources in response to changing conditions. Purohit and Vyas (2025) review how quantum machine learning algorithms might enhance QKD protocols by dynamically adjusting basis choices or error correction based on learned patterns in the quantum channel.

**More Comprehensive Noise and Attack Models:** Future studies are likely to develop more comprehensive stochastic models that incorporate multiple noise sources and attack vectors simultaneously. Instead of treating, for example, dark counts, photon loss, and polarization drift separately, a unified model (possibly a higher-dimensional Markov process or a multi-factor OU process) could capture their joint effects on the quantum state. This is complex, but as our ability to collect data from quantum devices improves, multi-factor models will become feasible to calibrate. Additionally, non-Markovian models are a frontier area: tackling environments with memory might involve using colored noise spectra, autoregressive models, or even combining deterministic chaos theory with stochastic processes to capture complex noise dynamics. Developing analytic methods or approximations for non-Markovian quantum noise (perhaps using perturbative expansions or reservoir engineering concepts) will enhance the realism of our security assessments. We also see potential in applying quantum stochastic calculus and quantum noise theory to cryptography. For instance, quantum Poisson processes or quantum Langevin equations could model the interaction of single photons with a fluctuating environment at a level that classical analogs cannot. This line of research could bridge the gap between abstract security proofs and hardware-specific noise characteristics, ensuring that every relevant physical effect is accounted for in the models.

**Efficiency and Scalability of Stochastic Methods:** On the practical side, future research will focus on making stochastic modeling techniques more efficient and scalable[10]. One direction is the use of importance sampling and variance-reduction techniques in Monte Carlo simulations for quantum cryptography, to get reliable estimates of failure probabilities (which are typically extremely small) without needing an astronomical number of trials. Another direction is developing analytical bounds that can replace brute-force simulation; for example, using concentration inequalities or large-deviation theory to bound the tail probabilities of error processes in QKD[10]. There is also interest in specialized hardware acceleration[10] (e.g., using quantum computers or specialized classical processors) for simulating stochastic processes. Some studies propose quantum algorithms that provide quadratic speedups in sampling stochastic processes. If such algorithms mature, they could allow real-time predictive modeling: a quantum computer could potentially simulate the next-hour noise evolution of a quantum channel faster than a classical computer, enabling proactive adjustments to the cryptographic protocol. Lastly, scalability is crucial for quantum networks: as we go from point-to-point QKD links to multi-node quantum networks[17][11], the complexity of modeling network-wide stochastic processes (including network traffic patterns, multiple eavesdroppers, etc.) grows. Research on stochastic network theory for quantum communications analogous to classical network queuing theory but with quantum constraints will be vital. Early work on QKD network routing using deep reinforcement learning hints at strategies to handle this complexity; continued progress could lead to robust quantum network simulators that guide deployment of global-scale quantum-secured networks[11].

**Integration with Quantum Error Correction and Fault Tolerance**: Stochastic process techniques will likely play a role in the next generation of quantum cryptographic hardware, particularly by informing the design of quantum error correction (QEC) codes and fault-tolerant protocols. QEC is essentially a way to counteract stochastic errors by adding redundancy. By understanding the statistical profile of errors (e.g., whether errors are predominantly $\sigma_z$ phase flips with a certain autocorrelation time), one can tailor QEC codes that target those error patterns. The future development of error correction methods for cryptography will benefit from stochastic modeling of error bursts and correlations. For example, if a stochastic model predicts that certain error events come in bursts, interleaving of codeword bits or using code designs that can correct burst errors would be advantageous[1]. Moreover, the decoder of a QEC code can utilize a probabilistic model of the noise (derived from a stochastic process) to perform maximum-likelihood error correction. Research in this vein could improve the efficiency of QKD over noisy channels by proactively correcting errors in a way that traditional QKD post-processing (which typically assumes i.d. errors) cannot.

In conclusion of this section, the limitations of current stochastic modeling in quantum cryptography are being actively addressed by a combination of more adaptive modeling, advanced computational methods, and deeper integration of physical reality into the models. The field is moving toward a more holistic approach: not viewing stochastic processes in isolation, but as part of a larger closed feedback loop wherein the quantum system, the adversary, and the cryptographic protocol all interact. By continuing to refine models and methods – with help from the latest in machine learning, quantum

computing, and classical stochastic analysis – researchers aim to ensure that the next generation of quantum cryptographic systems remains secure even under the complex, dynamic conditions of the real world[1].

## 6. Conclusion

This review has examined the multifaceted role of stochastic processes in quantum cryptography and highlighted how randomness and uncertainty can be harnessed to bolster security. Key findings include the insight that *Markovian models* and master equations provide a tractable way to analyze quantum noise and decoherence in protocols like QKD[1], while more complex processes (e.g., Ornstein–Uhlenbeck noise and Hidden Markov Models) can capture realistic temporal correlations and hidden attack strategies that simpler models miss. By analyzing these models, we saw improvements in understanding the *noise-induced error rates, secret key rate calculations, and eavesdropper detectability* in various quantum cryptographic schemes. We also discussed how stochastic modeling feeds into formal security proofs by quantifying the uncertainty (through entropy measures) and enabling rigorous statements about a protocol's security in a composable framework. However, our review also underscores important limitations[6][4]. No model is a perfect mirror of reality: mismatches between assumed stochastic behavior and actual quantum device behavior can lead to overly optimistic or pessimistic security estimates. We pointed out the challenges of computational complexity and the difficulties in estimating model parameters accurately in a quantum setting with limited data. These limitations temper the immediate optimism and call for cautious interpretation of any model-driven result. Notably, the security guarantees derived from stochastic models are only as reliable as the models themselves. Looking ahead, we have identified several promising directions for future research. One prominent theme is the convergence of quantum cryptography with modern machine learning and optimization techniques, which could enable adaptive security measures that learn from and respond to their environment in real time[6][4]. Quantum communications can benefit from the progressive advances in quantum hardware, networking, and error correction, thereby raising the probabilities of large-scale quantum communication networks. In future scenarios of these technologies, stochastic models will be of paramount importance to enhance the performance and security aspects and handle the heterogeneities found in the physical implementation of quantum cryptographic systems.

## Declaration

The authors confirm that AI-based language-assistance tools (e.g., Grammarly, ChatGPT, and comparable software) were used exclusively for grammar correction and formatting support. No scientific content, interpretation, or originality of the research was affected by these tools.

## References


1. Hughes, R.J., et al. *Quantum cryptography over underground optical fibers*. in *Advances in Cryptology—CRYPTO'96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings 16*. 1996. Springer.

2. Padamvathi, V., B.V. Vardhan, and A. Krishna. *Quantum cryptography and quantum key distribution protocols: A survey*. in *2016 IEEE 6th international conference on advanced computing (IACC)*. 2016. IEEE.

3. Shakhmuratov, R., A. Zinnatullin, and F. Vagizov, *Cryptography with stochastic photons*. Europhysics Letters, 2024. **147**(3): p. 38001.

4. Ullah, R., et al., *Intelligent decision making for energy efficient fog nodes selection and smart switching in the IOT: a machine learning approach*. PeerJ Computer Science, 2024. **10**: p. e1833.

5. Corner, C., et al., *Randomness in cryptography.* IEEE Security & Privacy, 2006. **4**: p. 64-67.

6. Ayub, N., et al., *Forecasting Multi-Level Deep Learning Autoencoder Architecture (MDLAA) for Parametric Prediction based on Convolutional Neural Networks*. Engineering, Technology & Applied Science Research, 2025. **15**(2): p. 21279-21283.

7. Hughes, R.J., et al. *Quantum Cryptography*. 1995.

8. Schindler, W., K. Lemke, and C. Paar. *A stochastic model for differential side channel cryptanalysis*. in *Cryptographic Hardware and Embedded Systems–CHES 2005: 7th International Workshop, Edinburgh, UK, August 29–September 1, 2005. Proceedings 7*. 2005. Springer.

9. Brands, S. and R. Gill, *Cryptography, statistics and pseudo-randomness (part I)*. Probability and mathematical statistics, 1995. **15**: p. 101-114.

10. Shah, S., et al., *A flexible and lightweight signcryption scheme for underwater wireless sensor networks.* Scientific Reports, 2025. **15**(1): p. 13511.

11. Sarwar, N., S. Al-Otaibi, and A. Irshad, *Optimizing Breast Cancer Detection: Integrating Few-Shot and Transfer Learning for Enhanced Accuracy and Efficiency.* International Journal of Imaging Systems and Technology, 2025. **35**(1): p. e70033.

12. Shaked, M. and J.G. Shanthikumar, *Stochastic orders and their applications.* (No Title), 1994.

13. COSTA, A.D.Q., A.D.A.B. NETO, and C.A.S. DE ALMEIDA, *VII OFICINA NACIONAL DE TEORIA QUÂNTICA DE CAMPOS VII NATIONAL WORKSHOP ON QUANTUM FIELD THEORY.*

14. Sarwar, N., et al., *Skin lesion segmentation using deep learning algorithm with ant colony optimization.* BMC Medical Informatics and Decision Making, 2024. **24**(1): p. 265.

15. Gennaro, R., *Randomness in cryptography.* IEEE security & privacy, 2006. **4**(2): p. 64-67.

16. Bielecki, T.R., J. Jakubowski, and M. Niewęgłowski, *Structured dependence between stochastic processes*. Vol. 175. 2020: Cambridge University Press.

17. Unnisa, Z., et al., *Impact of fine-tuning parameters of convolutional neural network for skin cancer detection*. Scientific reports, 2025. **15**(1): p. 1-23.

18. Muhammad, A.S., et al., *Recent Advances in U-type hexagonal ferrites: Synthesis, Characterizations, Magnetic and Absorption Properties.* Hybrid Advances, 2024: p. 100324.