

Secure Key Relaying in Quantum Key Distribution Networks with Malicious Relay Nodes

Zarna Dinesh Solanki

Birla Institute of Technology and Science, Pilani

Aayush Jain

Birla Institute of Technology and Science, Pilani

Adwait Gondhalekar

Birla Institute of Technology and Science, Pilani

Vijay Shankar A

Birla Institute of Technology and Science, Pilani

Ashutosh Bhatia Bhatia

`ashutosh.bhatia@pilani.bits-pilani.ac.in`

Birla Institute of Technology and Science, Pilani

Sainath Bitragunta

Birla Institute of Technology and Science, Pilani

Research Article

Keywords: Quantum Key Distribution, QKD networks, malicious relay nodes, Shamir's Secret Sharing, secure key relaying, quantum-safe communication

Posted Date: October 15th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10130228/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Secure Key Relaying in Quantum Key Distribution Networks with Malicious Relay Nodes

Zarna Dinesh Solanki², Aayush Jain¹, Adwait Gondhalekar¹,
Vijay Shankar A¹, Ashutosh Bhatia^{1*}, Sainath Bitragunta²

^{1*}Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani Campus, Pilani, 333031, Rajasthan, India.

²Department of Electrical and Electronics Engineering, Birla Institute of Technology and Science, Pilani Campus, Pilani, 333031, Rajasthan, India.

*Corresponding author(s). E-mail(s):

ashutosh.bhatia@pilani.bits-pilani.ac.in;

Contributing authors: p20241008@pilani.bits-pilani.ac.in;

h20230083@pilani.bits-pilani.ac.in; h20230089@pilani.bits-pilani.ac.in;

vijay.shankar@pilani.bits-pilani.ac.in;

sainath.bitragunta@pilani.bits-pilani.ac.in;

Abstract

Secure key distribution is crucial for maintaining communication confidentiality in networks with multiple communicating partners. Asymmetric key algorithms are vulnerable to quantum attacks because of the computational advantage offered by quantum computers, whereas symmetric key algorithms with sufficiently large keys remain comparatively more resistant. Quantum Key Distribution (QKD) has emerged as a promising quantum-secure key distribution technique based on the principles of quantum physics. However, practical QKD networks often rely on relay nodes to extend communication distance, and malicious relay nodes can compromise quantum keys during the relaying process. This study proposes a secure key relaying approach based on Shamir's Secret Sharing to mitigate this vulnerability. The proposed method uses a probabilistic behavioural model to assess relay nodes according to their curiosity and collaboration tendencies. By splitting a quantum key into multiple shares and routing them through paths with minimum compromise risk, the approach reduces exposure to malicious or colluding relay nodes. The proposed algorithm assigns risk

to network paths by evaluating node-level curiosity and collaboration potential, determines the appropriate number of shares, and selects secure routing paths to minimise key compromise. The study further analyses the parameters influencing the ideal number of shares for a given network, thereby offering a resilient mechanism for quantum-safe communication in QKD networks with malicious relay nodes.

Keywords: Quantum Key Distribution, QKD networks, malicious relay nodes, Shamir’s Secret Sharing, secure key relaying, quantum-safe communication

1 Introduction

In the digital age, secure communication is paramount for protecting sensitive data across networks. Traditional cryptographic systems rely heavily on computational hardness assumptions, particularly in asymmetric encryption schemes. However, the advent of quantum computing threatens these assumptions, potentially undermining widely used security protocols. This risk has spurred parallel efforts in advancing post-quantum cryptography and quantum-safe communication techniques.

The emergence of quantum computing and its application to tackle theoretically challenging issues, such as prime factorisation and discrete logarithms, has put the current generation of encryption systems at risk of being cracked. Given the efficiency with which quantum computers can perform prime factorisation, asymmetric encryption has the highest probability of being cracked among symmetric and asymmetric encryption techniques. The National Institute of Standards and Technology (NIST) predicts that full-scale quantum computers capable of cracking asymmetric cryptography will be available by 2030. Therefore, it is a race between quantum computing and cryptography researchers working to advance their respective fields. In light of this, work on Post-Quantum Cryptography standards is underway and progressing quickly to lessen the impending threat.

QKD utilises the principles of quantum physics to generate and distribute secure keys, employing light photons to transmit the secret key between two communicating parties, thereby representing a significant shift from conventional secure communications. Since the observation of a quantum signal results in a change in its state, suggestive of an interception, the inherent characteristic of this technology is its ability to detect eavesdropping or interception. Despite the promising aspects of QKD systems, their implementation is not as simple as it may appear; the orientation of the photon is crucial for conveying information and sustaining this orientation over long distances—even using optical fibres—is a challenge in and of itself.

Incorporating several relay nodes into larger networks is a natural solution to this problem. These nodes duplicate the quantum signals, facilitating the distribution of keys across greater distances [1]. However, significant risks are associated with employing many relay nodes, including the potential for alteration or interception of the key. The presence of malicious relay nodes in a QKD network further exacerbates the problem since they can partially access the quantum key as it passes through them

[2]. This risk highlights a serious flaw that could jeopardise the system’s security since these nodes might attempt to replicate the encryption key alone or in collaboration. While QKD Networks offer information-theoretic security, it is now well known that they are not completely free from attacks [3, 4]. In the case of relay nodes, one must consider the possibility of collaborative attacks, such as black hole and grey hole attacks [5], making dealing with a malicious node even more significant.

Recent deployments underscore the practical scalability of trusted-relay QKDNs at carrier grade. In 2025, China reported the CN-QCN backbone spanning over 10,000 km with 145 backbone nodes and integrated satellite ground stations [6]. Alongside scale, network-level constraints persist—especially routing under key scarcity, buffer dynamics, and the operational risks of trusted nodes [7]. These realities motivate our focus on secure key relaying with malicious relays and robustness beyond purely topological guarantees.

This study attempts to address the vulnerabilities caused by malicious nodes in QKD networks and tries to resolve them using an algorithm based on Shamir’s secret sharing (SSS) method. According to this technique, the secret—in our example, a quantum key—is divided into multiple pieces and transmitted via various paths in the network; no single share discloses any information about the secret until a node gathers a certain threshold number of shares. We develop an algorithm that probabilistically models every node in the network, considering the entire network state. This algorithm considers each node’s curiosity in accessing or decoding information and its collaboration with other nodes in the network to obtain key shares. Next, the risk of each node breaking the secret is assigned. The aim is to reduce the likelihood that any share will be intercepted or compromised by the relay nodes by objectively assigning a risk factor to each path, taking into account the hazard of each node along that path. Ultimately, for the key transmission, the least risky paths are considered, and the risk of each path is determined based on the probabilistic behaviour of its constituent nodes.

To address these vulnerabilities, this paper proposes a secure key relaying technique using Shamir’s Secret Sharing. By splitting the key into multiple parts and intelligently routing them based on the behaviour of relay nodes, our method limits exposure even in adversarial environments.

2 Quantum Key Distribution

Quantum Key Distribution (QKD) enables two distant parties to establish a shared secret key with information-theoretic security by exploiting fundamental principles of quantum mechanics, such as the disturbance caused by measurement and the no-cloning theorem [8]. Unlike classical cryptographic schemes that rely on computational hardness assumptions, QKD guarantees that any eavesdropping attempt on the quantum channel introduces detectable errors, allowing legitimate parties to abort key generation when the channel is compromised. Practical QKD systems predominantly rely on photonic quantum states transmitted over optical fiber links, which offer higher secret key rates and operational stability compared to free-space or satellite-based QKD, albeit with limited transmission distance due to photon loss and decoherence [9].

To overcome the inherent rate–distance trade-off, modern QKD networks employ trusted relay architectures, in which keys are relayed hop-by-hop across multiple intermediate nodes using a combination of quantum key generation and classical post-processing. While this approach enables scalable, carrier-grade QKD deployments, it introduces a fundamental vulnerability: intermediate relay nodes gain access to key material during the relaying process, making the over

3 Enhancing QKD Systems Through Key Relaying

While offering unprecedented security based on the principles of quantum mechanics, QKD protocols face significant practical limitations, particularly in terms of key generation or secret key generation rate, as well as the correlation of this rate with the transmission distance [3]. The key rate K is a crucial parameter that measures the effectiveness and security of the key generation procedure [10]. It denotes the speed at which two people, Alice and Bob, may generate secure cryptographic keys when an eavesdropper, Eve, is present. The significance of K lies in its direct impact on QKD systems’ practical deployment and robustness. The key generation rate decreases significantly as the distance between the two communicating parties increases [11]. This reduction is primarily due to photon attenuation over extended optical fibre channels, resulting in higher signal loss and lower detection probabilities as the distance increases [12]. Photon loss limits the effective transmission of quantum states, resulting in an exponential decline in the key generation rate with increased separation [13]. Thus, overcoming this rate-distance trade-off remains a critical challenge in scaling QKD systems for secure long-distance quantum communication.

To overcome these limitations, key relaying in QKD networks emerges as a viable solution [14]. By replacing a single long-distance quantum channel with a series of shorter, interconnected channels through intermediate nodes, key relaying significantly enhances the effective range and key rate of QKD systems [15]. This approach utilises either quantum repeaters or quantum relays to facilitate the secure transmission of quantum keys across extended distances [16].

Quantum relays, which are more technologically feasible than quantum repeaters, operate by securely extending the reach of QKD without requiring the storage and manipulation of quantum states, which are necessary for quantum repeaters [17]. In practical implementations, relaying the secret key from the source to the destination hop-by-hop requires daisy-chaining of quantum relays. This involves each relay performing two independent QKD operations: one with its preceding node and another with its succeeding node [18]. Consequently, each relay holds two secret keys: one shared with the node before it and another with the node after it.

The key relaying process starts with the first relay creating a joint key by performing an XOR operation between the service key and its other secret key [19]. The service key is the key that both the source (Alice) and destination (Bob) will eventually use to encrypt and decrypt messages exchanged over a classical channel. The relay transmits this joint key to the next relay through a classical communication link. Successive relays continue this pattern: they receive a joint key, extract the service key

by XORing it with their previous-hop secret key, and generate a new joint key using their next-hop secret key, which is then sent to the next relay in the chain.

This method concludes at the final relay, which sends the last joint key to Bob. Bob extracts the service key by performing an XOR operation with the secret key he generated through QKD with this final relay. It is crucial to note that throughout this relay process, the integrity and secrecy of the service key depend on the trustworthiness of the intermediate relays [20]. Since the key is effectively in plaintext form at each relay stage, the security of the entire communication depends critically on each relay being secure and trusted not to disclose the key to any unauthorised party [2].

Through such a relay mechanism, QKD networks effectively extend their operational range while mitigating the rate-distance limitation inherent in direct QKD transmissions [21]. This method enhances the practical applicability of QKD systems across greater distances and maintains the high-security standards essential for quantum communications. We emphasize that relayed QKDNs forward *keys* hop-by-hop over classical links (via XOR/key-transport), rather than duplicating quantum states end-to-end. For broader architectural context, relayed designs using trusted nodes remain dominant in carrier-grade deployments, whereas switched designs aim for end-to-end paths but impose tighter hardware/scheduling constraints [22].

4 Shamir's Secret Sharing

Shamir's Secret Sharing [23], developed by Adi Shamir in 1979, is a cryptographic method designed to divide a secret, such as a cryptographic key, into multiple parts or shares. The scheme is based on polynomial interpolation principles, allowing a secret S to be split into m shares so that any k out of m shares can reconstruct the secret. The setup ensures that possessing fewer than k shares provides no information about the secret, thereby safeguarding it unless it meets the threshold k .

The mathematical foundation of Shamir's Secret Sharing utilises polynomial interpolation in a finite field $\mathbb{F}_p$, where p is a prime number larger than the number of shares m and the secret size. To implement this, a polynomial $f(x)$ of degree $k - 1$ is constructed, where:

$$f(x) = S + a_1x + a_2x^2 + \dots + a_{k-1}x^{k-1} \quad (1)$$

In this polynomial, S is the secret to be protected, and the coefficients $a_1, a_2, \dots, a_{k-1}$ are randomly selected from $\mathbb{F}_p$. The polynomial is evaluated at distinct points $x_1, x_2, \dots, x_m$, generating m shares in the form $(x_i, f(x_i)) \forall i \in [1, m]$. Using techniques like Lagrange interpolation, the polynomial $f(x)$ and thus the secret S can be uniquely determined from any k points. The interpolation formula given k points is:

$$f(0) = \sum_{i=1}^k f(x_i) \prod_{1 \leq j \leq k, j \neq i} \frac{-x_j}{x_i - x_j} \quad (2)$$

Here, $f(0)$ directly provides the secret S , as it corresponds to the constant term of the polynomial.

In cryptographic applications, Shamir's Secret Sharing is particularly valuable for distributing a key or sensitive information across multiple parties, ensuring the

integrity and availability of the key remain intact even if some shares are compromised or lost. For instance, in environments where a cryptographic key must be stored securely without entrusting it to any single party, such as in a distributed network of servers, Shamir's scheme offers a practical solution by distributing the key across multiple locations. The scheme's flexibility also makes it useful for secure multiparty computations and enhancing security protocols in technologies like blockchain, which can provide robust security measures for managing digital assets and conducting transactions securely. Additionally, the scheme finds applications in disaster recovery strategies, ensuring data recovery through key reconstruction from shares stored in geographically diverse locations, thus protecting data against localised catastrophic events.

Shamir's Secret Sharing is recognised as quantum-safe primarily because it relies on polynomial interpolation, a mathematical process not based on the number-theoretic assumptions that quantum algorithms like Shor's algorithm exploit. This characteristic is vital for QKD network applications. The quantum safety of Shamir's Secret Sharing stems from the fact that it does not depend on the difficulty of factoring large numbers or computing discrete logarithms, which are computational problems that quantum computers can solve efficiently.

In contrast, the security of Shamir's Secret Sharing is based on the complexity of solving a system of linear equations to reconstruct a polynomial in a finite field, a task for which no quantum speedup is known. This property ensures that even with advancements in quantum computing, the scheme remains resistant to decryption by quantum methods. Therefore, integrating Shamir's Secret Sharing into QKD systems ensures that even if the key distribution process involves multiple stages or nodes, the system retains robust protection against quantum computing threats.

By utilising Shamir's Secret Sharing to manage or distribute keys within a QKD network, the complete security architecture maintains consistency with the quantum-safe principles underlying the quantum channels. This approach not only preserves the integrity and purpose of using QKD to establish and distribute cryptographic keys securely but also extends quantum resistance throughout the network's infrastructure, safeguarding against potential future cryptographic threats while ensuring comprehensive network-wide protection.

Proposition 1 (Compromise probability under (k, m) sharing) *Let X_i be the indicator that share i is intercepted by M under placement policy π . Then*

$$Q_{\Delta}(\mathcal{P}, \pi) = \Pr\left(\sum_{i=1}^m X_i \geq k\right) = \sum_{j=k}^m \binom{m}{j} p_j(\mathcal{P}, \pi), \quad (3)$$

where p_j is the probability exactly j shares are intercepted.

Union bound / inclusion-exclusion tightening. With $A_i = \{X_i = 1\}$,

$$Q_{\Delta} \leq \sum_{j=k}^m \sum_{\substack{S \subseteq \mathcal{S}: \\ |S|=j}} \Pr\left(\bigcap_{i \in S} A_i\right), \quad (4)$$

$$Q_{\Delta} = \sum_{j=k}^m (-1)^{j-k} \sum_{\substack{T \subseteq S: \\ |T|=j}} \binom{|T|-1}{k-1} \Pr\left(\bigcap_{i \in T} A_i\right). \quad (5)$$

Node-/group-disjoint placements reduce $\Pr(\cap_{i \in S} A_i)$, tightening (4)–(5).

Moreover, the bounds in (4)–(5) show how reducing overlap between share-carrying paths (node-/group-disjointness) decreases joint interception probabilities, thereby tightening the compromise bound and motivating our disjoint-routing preferences.

5 Related Work

Fujiwara et al. [24] have presented a QKD-based key management framework that utilises password-based authentication techniques, along with Shamir’s Secret Sharing, to protect a distributed network from malicious nodes. Strongly depends on the password-based authentication and the security offered by QKD. However, the method does not account for the event that the QKD nodes can also be malicious. It also relies too heavily on the security of the data owner node.

Trusted-relay architecture is increasingly studied with node credibility and placement considerations. Reliability-/trust-aware repeater placement integrates trust scores into path selection to maximize secure connectivity with limited TRNs. Complementary backbone proposals introduce hybrid trusted/untrusted relays augmented with a quantum key pool (QKP) for cost-optimal provisioning.

The Review [25] clearly indicates that key distribution in a QKD network is inherently different from classical network routing, mainly due to the unique requirement to preserve the secrecy of the key at all costs. Kong conducts an extensive study on how the classical and quantum channels of the network need to be integrated to deliver the key on multi-hop paths, while maintaining absolute trust in the intermediate relay nodes. These considerations lead to a few operational challenges, like the necessity for two channels (quantum and classical) and the dependence of secret key rate as a bottleneck to the overall network performance, and these key takeaways from Kong’s work highlight the significant differences between classical and QKD routing and the considerations necessary for their fusion. The work is well established and even provides information on the protocols used in QKD node communication, the primary target of Eavesdropping/Key-recovery attacks by an adversary in these systems.

The proposed adaptive stochastic routing algorithm by Le Quoc, Bellot, and Demaille [26] is complex for an eavesdropper to detect, thereby increasing the overall security of the network. The method is adaptive in nature, i.e. they change their key routes depending on the current state of the network. Their approach could be more robust against eavesdroppers, and the assumption of being able to partially compromise the network nodes is more realistic, providing a valuable practical insight into quantum network security issues, where full trust in the nodes cannot always be ensured.

The proposed multipath multi-segment QKD routing algorithm by Liu, Che, Xie, and Dong [27] is efficient in terms of achieving greater distance while maintaining

higher security compared to the single-path/single-segment QKD network. The multi-segment multipath approach is much more secure compared to a single path approach, as the network has many other independent paths, which are secure too. This provides a very important concept which states that even if a node is compromised, the security of the network is still not at risk. The assumption of their work that they segment networks is reasonable. This research is innovative because of the way it approaches the QKD network concept, which incorporates a property of trust. They fuse a high level of trust for node reliability into the model with the old assumption of the necessity of key freshness, which could be a good approach, and the results of the work show that this is the case.

The research conducted by Wenning et al. [28] demonstrates buffer-aware demand routing of secret keys in QKD networks. The work focused on optimising the approach to routing strategies to enable an efficient distribution of secret keys. They focused on the buffer capacity of the nodes to prevent network congestion and latency. The results showed that, with the right approach in this regard, there is a good chance of improving reliability in a QKD network. The author even suggests the possible implementation of advanced buffer management techniques in the future.

Beyond deterministic policies, learning-based controllers have emerged for QKDN routing. A Q-learning router adapts to residual-key imbalances and topology-induced congestion, improving delay/failure trade-offs under realistic loads [29]. Our formulation differs by explicitly modeling colluding/malicious relays during key-relay decisions.

Wang and Liu [30] discuss the security issues with trusted relay nodes in QKD networks. Their analysis reveals that trusted relay nodes are susceptible to cascading attacks, which can compromise the network's overall security. The research aims to explore all possible angles from which an attack can be launched and its resulting impact. It also proposes several methods for securing the trusted relay nodes in a QKD network from all possible angles, thereby ensuring the overall security of the network. Wang and Liu [30] show the proof for the assumed security in trusted relay nodes. The results of the work are practical and demonstrate a real-world application. The work demonstrates QKD network complexity management via trusted relay nodes, but it is a relatively new area in QKD networks and has not been extensively explored, so the thoroughness of the work is commendable. The model can be reused in many other instances and areas of work.

The research conducted by Shafie et al. [31] presents a new secret-key-aided scheme designed to enhance security in untrusted relay nodes of a QKD network. The work outlines the key assumptions, which include the utilisation of classical cryptographic techniques and their integration with the QKD mechanism. The results show that this method is easily applicable to a QKD network and even provides an estimate of the overhead involved, assuming a secret key is available in the model. The work is thorough and can be applied to multiple uses; however, it is a newly discovered area of research, and not much detail can be provided at this stage. The model could be reused in real-world applications.

Phoenix and Barnett [14] were able to show the feasibility of end-to-end secure communication over a QKD network with the aid of relay nodes. The research outlines

the operating mechanisms required for a QKD network to function with the application of relay nodes. The research provides an insight into a possible use case, its key assumptions, the overhead involved in the model, and even theoretical and real-life challenges in deployment. The work done by Phoenix and Barnett [14] is reusable, practical, and even thorough.

Grillo, Dowhuszko, Khalighi, and Hämäläinen [32] have presented an algorithm designed to address the issue of resource allocation in a QKD network. The resource allocation mechanisms are non-trivial due to the high security requirements in a QKD network. The work by Grillo, Dowhuszko, Khalighi, and Hämäläinen [32] demonstrates that, with the right approach, even under the constraints of resource allocation, a secure QKD network with optimal resource allocation is feasible. This research work is reusable and provides both theoretical and practical knowledge.

Cao et al. [33] have presented a method that utilises trusted relay nodes to enhance the overall network performance and key generation rate. This is a new method that is not yet in use, but the work provides both theoretical and practical knowledge of the new method. The proposed method is robust and focuses not only on the key generation rate but also on enhancing the overall network's performance. The work done is practical and well-researched, and it is even illustrated with a real-world application. The re-usability of the model is possible, but also in very specific use cases.

Zhao et al. [34] conducted a study on the application of machine learning algorithms in QKD networks that utilise trusted relay nodes. The use of AI is a novel technique in this field. The work done is non-trivial, as the researchers applied known algorithms to a new field and provided both theoretical and practical performance of the method. The results demonstrate an increase in the key generation rate and a more effective approach for dynamically changing routing in the network. The study is unique and also provides a practical use case. The work is reusable.

The routing algorithm proposed by Kong [35] uses trusted relay nodes to provide an approach which minimises latency and maximises key throughput. The work is a new and innovative approach to the problem of QKD network routing and also shows a real-world application with theoretical and practical aspects. The work done is reusable and has good practical use-case examples, and it is well-established. The study provides multiple results which are well established by the research conducted.

The study done by Chen, Chen, Chen, and Zhao [36] on the scalability of QKD networks which use trusted relay nodes is a good and reliable use case in the real world. Scaling such a network is very difficult, and the work provides an innovative solution which can be directly applied with the provision of knowledge on the issue faced. The work is reusable and well-established with a real-world application.

The work done by Wang and Huberman [37] provides important theoretical and practical insights into environmental factors affecting trusted relay QKD networks. The work is non-trivial as a new problem is being approached and the research done provides practical knowledge on such issues and knowledge on how the theory works on such networks, and this provides both the theoretical and the practical application. The results are applied and utilised in a real-world setting. The work is reusable, but only for environmental-specific changes in QKD networks.

6 Behavioral Modeling of Relay Nodes

Two characteristics – curiosity and collaboration – define the behavior of a relay node in the network. These characteristics play a significant role in determining the risk factor associated with a node in the network. Based on the risk assessment corresponding to all nodes in the network, the source determines the number of shares to split the key and the paths they will follow.

Definition 1 (Curiosity) *Curiosity* denotes the probability that any node in the network would try to decode/break the secret, given that it has access to all its shares.

It is an inherent property of any relay node to be curious about the data (secret in our case) that it relays and tries to eavesdrop on it to satisfy its curiosity. However, the level of curiosity of each node can vary, and this varying level of curiosity determines the amount of effort the node is willing to put into deciphering the secret transmitted through it. A critical assumption we make is that for any node to decipher the secret, it must first gather or possess all the secret shares.

Definition 2 (Collaboration) *Collaboration*(A, B) indicates the probability that node A receives a share of message given that node B has that share (as node B lies along the path chosen by the source).

Collaboration models the likelihood that a node not along the path the source took to route a share can gather that share. We consider that this likelihood is independent across shares, that is, independent of previous collaboration. When nodes exhibit collaborative behaviour, they are prepared to help one another decode the secret by sharing (communicating) the information they eavesdropped on with other nodes. Collaboration intent is mutual between parties, meaning $Collaboration(A, B) = Collaboration(B, A)$. Each node can have varying levels of collaboration with the other nodes. Curious and collaborative behavior are independent of each other. Some non-curious nodes may be more collaborative with other nodes. They are not interested in decoding their message but are willing to share their information with other nodes. Some nodes may be highly curious but not collaborative, i.e., they want to decode the secret independently with the shares they gathered.

We consider two types of network models: deterministic and probabilistic, depending on whether the assignments of curiosity and collaboration to each node in the network differ.

In addition to eavesdropping and attempting to obtain the key, one must consider two very important types of attacks that can be carried out by malicious relay nodes: the Black Hole and Grey Hole attacks, respectively [38]. These attacks can be carried out by either individual or through collaborations. The Black Hole attack would simply drop the message packets - also known as a full packet drop attack - and can be regarded as a type of Denial of Service attack [38]. A more sinister attack is the Grey Hole attack, which selectively drops packets and is hence known as a partial packet

drop attack [38]. In this case, these nodes are difficult to detect because they behave like normal nodes but intermittently drop packets. It is not difficult to see that these attacks can threaten the network under consideration by preventing key information from reaching the destination node, further reinforcing the importance of combating malicious nodes.

6.1 Deterministic Model

The curiosity and collaboration values are assigned discretely to each node in a deterministic model, i.e., the curiosity of a node may either be 0 or 1, and the collaboration will also be either 0 or 1. A node may be fully curious, noncurious, collaborative, or non-collaborative. To explain this model, we consider one behavior at a time.

6.1.1 Curiosity

In this model, the source attempts to identify a route to the destination that involves only noncurious nodes. If a suitable path is discovered, the key is forwarded along this route, ensuring no curious nodes can access it. However, the key must be divided into multiple shares if such a path cannot be found. The source now examines an induced network comprised solely of curious nodes while preserving the relationships of paths involving noncurious nodes, which poses no issues. This consideration also applies to scenarios where a node views all other nodes as curious.

Consequently, the source must determine which paths to select and the number of shares to generate. A straightforward approach involves identifying paths such that any node appears precisely once in all the selected paths leading to the destination within the induced network. The key has to be divided into several shares equal to the number of such paths found, with each share transmitted along a distinct path. This method ensures that no node possesses all the shares.

In this context, we require two shares and two node-disjoint paths (except the source and destination) to transmit the shares. If such paths do not exist, it implies that specific nodes participate in all identified paths. In this situation, additional paths must be explored. We consider disjointness within the induced network, and noncurious nodes may receive all the shares.

Theorem 2 *Let G be a finite undirected graph and let s and t be two distinct non-adjacent vertices. Exactly one of the following holds:*

1. *There exist at least two internally vertex-disjoint s - t paths; or*
2. *There exists a vertex $v \notin \{s, t\}$ that lies on every s - t path.*

Proof By the vertex version of *Menger's Theorem*, the maximum number k of pairwise internally vertex-disjoint s - t paths equals the size of a minimum s - t vertex-cut $C \subseteq V(G) \setminus \{s, t\}$.

- If $k \geq 2$, then no single vertex can belong to every s - t path, establishing Item(1).

- If $k < 2$, then $k = 1$, so $|C| = 1$. Let $C = \{v\}$. Removing v disconnects s from t ; hence v lies on every s - t path, establishing Item(2).

Thus, the theorem follows directly from Menger's Theorem. $\square$

6.1.2 Collaboration

Now, the source also considers the collaborative behavior of nodes. The source models pairs of nodes as collaborating or not; such modelling results in *collaborating groups*. A *collaborating group* consists of nodes that directly collaborate or have a sequence of nodes through which they collaborate indirectly. If any node in the collaborating group gets a share, all the other members are notified of that share. It is important to note that the resulting collaborative groups are distinct and do not overlap. In this model, there may be collaborative groups in which none of the members are curious. However, if at least one member of a collaborative group is curious and participates in the collaboration process, then the curious member will also receive the key share. Thus, such groups are labelled as curious. The source creates an induced network of curious nodes but cannot overlook the members of curious, collaborative groups. Therefore, we classify all members of these collaborative groups as curious, regardless of whether they are inherently curious. Subsequently, an induced network of curious nodes is constructed. The node then seeks additional disjoint paths until no member of any curious, collaborative group is included in all of these disjoint paths. In other words, we are looking for **node-disjoint paths** that are also **group-disjoint**.

6.2 Probabilistic Model

The source node models the behavior of relay nodes probabilistically in this model every node's curiosity and collaboration values range from 0 to 1. For any node to break a key, it must first gather all the shares of the key. This process consists of two phases: gathering and decoding. The gathering phase involves a node collaborating with other nodes to gather shares it does not have (as it does not lie on those paths). The decoding phase depends on the node's curiosity, i.e., the effort it is willing to put into decoding.

By the probabilistic behavioral model, we need probabilistic measures for performance evaluation or comparison of various path choices and the number of shares. These measure the likelihood of adversaries succeeding (breaking the message) or the likelihood of the adversaries failing. First, we need to quantify each phase, which will finally lead to quantifying the final or overall performance measures.

Given a set of paths (routes taken by each share) S , with cardinality m , we can define the measures discussed below.

6.2.1 Gathering phase

Let $\mathcal{G}_A$ be the probability of a node having all the key shares. To calculate $\mathcal{G}_A$, we define $\mathcal{G}_A(i)$ as the probability that a malicious node A obtains the i^{th} share of the message. Assuming that the probability of obtaining a particular share is independent of obtaining other shares, the value of $\mathcal{G}_A$ can be calculated as:

$$\mathcal{G}_A = \prod_{i=1}^m \mathcal{G}_A(i) \quad (6)$$

A node may receive the i^{th} share directly (if it lies along that path) or collaboratively. If node A lies along the path, then $\mathcal{G}_A(i) = 1$. The gathering probability, instead, must rely on paths in which A does not lie, denoted by R . Now, $\mathcal{G}_A(i)$ is the probability that node A collaborates with at least one node in the set R defined below. Therefore:

$$R = \{P \in S \mid A \notin P\} \quad (7)$$

$$\mathcal{G}_A(i) = \begin{cases} 1.0, & A \in S_i \\ \left(1 - \prod_{B \in R_i} (1 - \text{Collab}(A, B))\right)^{\frac{|R|}{|S|}}, & A \notin S_i \end{cases} \quad (8)$$

Eqn. (8) contains a power factor $\frac{|R|}{|S|}$ to take into account other shares that may be received directly. For example, if node A receives 2 out of 3 shares directly, i.e. it lies on two of the paths in S , the effective “risk” of it receiving the third share is increased, which is considered by this power factor.

6.2.2 Breaking phase

Once an adversary gathers all shares, it must decode them to break the message. Let Q_A be the probability that node A decodes the message.

$$Q_A = \text{Curiosity}(A) \cdot \mathcal{G}_A \quad (9)$$

We must consider the aggregated breaking probability, Q , across the network. Q can be defined based on different measures discussed below. Let M_1 be the probability that at least one node in the network can break the secret.

$$M_1 = 1 - \prod_{A \in N} (1 - Q_A) \quad (10)$$

N is the set of all nodes in the network (excluding the source and destination). Similarly, let M_2 be defined as the maximum of all the breaking probabilities of nodes in the network. The value of M_2 is:

$$M_2 = \max(Q_A), \forall A \in N \quad (11)$$

We select M_1 as the aggregated breaking probability to maximize security.

$$Q = 1 - \prod_{A \in N} (1 - Q_A) \quad (12)$$

7 Methodology

The probabilistic behavioral model in Section VI yields node-wise share-gathering and decoding probabilities, which together determine the risk that malicious relays can reconstruct the key. We formalize this reconstruction risk using $Q_{\Delta}(S, \pi)$ from Proposition 1, which measures the probability that at least k of the m shares are intercepted under a given path set S and placement policy π . Accordingly, Section VII casts the routing-and-sharing design as an optimization problem (13) that trades off routing overhead $\text{Cost}(m, S)$ with compromise risk $Q_{\Delta}(S, \pi)$ (or its tractable surrogates), and then provides the algorithmic procedure used in our simulations.

7.1 Modeling Assumptions

The network model in our setup consists of two communicating parties, Alice and Bob. Alice is the sender, and Bob is the receiver. These two parties do not communicate via traditional channels and have no pre-shared secrets. In our network graphs, nodes 0 and $n - 1$ represent the sender and receiver, respectively. The sender relies on the network of relay nodes between it and the receiver to share and communicate the key.

Furthermore, the sender possesses complete knowledge of each relay node and its behavior within the network. Relay nodes accurately compress and forward the data they receive to the next node without any alterations. While relaying the data, a relay node may be curious and eavesdrop on the communication, eventually requiring the sender to break the key into multiple shares to ensure that the key is not directly accessible to any single relay node. In such a scenario, a relay node may also collaborate with its counterparts to gather all the key shares.

As per Shamir’s secret sharing, we consider a simplified scenario requiring all m shares to reconstruct the key; however, our approach can be generalised to require k out of m shares.

7.2 Algorithm

Since the deterministic model is a special case of the probabilistic model with all probabilities set to 0 or 1, we can utilise a common algorithm, seen in Alg. 1, to determine the optimal solution. The algorithm minimises the overall breaking probability, Q , to determine the optimal number of shares for a given network. This algorithm has a time complexity of $O(e^{|\mathcal{P}|} * n^2)$ where $\mathcal{P}$ is the set of simple paths in the network. The algorithm applies the below constraints:

1. There is no benefit of sending different key shares across the same path since all nodes along the repeated path now have an increased probability of decoding the key. Hence, we avoid using combinations with repetitions.
2. Similarly, breaking the key beyond $|\mathcal{P}|$ is not beneficial since the breaking probability increases, implying that $1 \leq m \leq |\mathcal{P}|$ where m is the optimal number of shares.

There may not always be an optimal solution possible given a particular network. For deterministic models, the absence of noncurious nodes with larger collaboration groups means that there may not be any set of paths that do not contain collaborative

Algorithm 1 Optimal Solution for Malicious Relay Nodes

Require: $\mathcal{P}$ is the set of simple paths

Require: *curiosity* is an array of decoding probabilities of each node

Require: *collaboration* is a matrix of collaboration probabilities of each node with other nodes

```
1: optimal_shares  $\leftarrow 0$ 
2: optimal_paths  $\leftarrow \phi$ 
3: max_q  $\leftarrow 1.0$ 
4: for  $m = 2$  to  $|\mathcal{P}|$  do
5:   optimized  $\leftarrow false$ 
6:   path_combinations  $\leftarrow \text{combination}(\mathcal{P}, m)$ 
7:   for chosen_paths  $\in$  path_combinations do
8:     path_q  $\leftarrow Q(\text{chosen\_paths}, \text{curiosity}, \text{collaboration})$ 
9:     if path_q  $<$  max_q then
10:      max_q  $\leftarrow$  path_q
11:      optimal_paths  $\leftarrow$  chosen_paths
12:      optimized  $\leftarrow true$ 
13:     end if
14:   end for
15:   if  $\neg$ optimized then
16:     return optimal_shares, optimal_paths
17:   end if
18:   optimal_shares  $\leftarrow m$ 
19: end for
20: return no_solution
```

nodes. Similarly, the network topology may also impact the existence of an optimal solution.

7.2.1 Optimal Solution for the Deterministic Model

In the deterministic model, it is essential to find paths such that no two paths contain the same collaborative group, i.e., we must find **node-disjoint paths** that are also **group-disjoint**. When collaboration does not exist in the network, the number of collaboration groups equals the number of nodes, n , in the network. Thus, for the deterministic model, Algorithm 1 can be simplified to Algorithm 2.

Design Objective

We cast the design as:

$$\begin{aligned} \min_{m, k, \mathcal{P}, \pi} \quad & \alpha \text{Cost}(m, \mathcal{P}) + (1 - \alpha) Q_{\Delta}(\mathcal{P}, \pi) \\ \text{s.t.} \quad & 1 \leq k \leq m \leq m_{\max}, \quad \lambda(\mathcal{P}) \geq k. \end{aligned} \tag{13}$$

Algorithm 2 Deterministic Model: Filtering Paths with Non-Consecutive Curious Nodes

Require: $\mathcal{P}$ is the set of simple paths

Require: CN is the set of curious nodes

Require: CG is a set of node groups whose members collaborate with one another

```
1:  $curious\_CG \leftarrow \{G \in CG \mid G \cap CN \neq \emptyset\}$ 
2:  $CG\_on\_paths \leftarrow \{(P, \{G \in CG \mid G \cap P \neq \emptyset\}) \mid P \in \mathcal{P}\}$ 
3:  $valid\_CG\_on\_paths \leftarrow \emptyset$ 
4: for all  $(P, groups) \in CG\_on\_paths$  do
5:    $labels \leftarrow [1 \text{ if } node \in CN \text{ else } 0 \text{ for each } node \in P]$ 
6:    $valid \leftarrow \text{true}$ 
7:   for  $i = 2$  to  $|labels|$  do
8:     if  $labels[i] = 1 \wedge labels[i - 1] = 1$  then
9:        $valid \leftarrow \text{false}$ 
10:      break
11:    end if
12:  end for
13:  if  $valid$  then
14:     $valid\_CG\_on\_paths \leftarrow valid\_CG\_on\_paths \cup \{(P, groups)\}$ 
15:  end if
16: end for
17: if  $valid\_CG\_on\_paths \neq \emptyset$  then
18:   for  $m = 1$  to  $|valid\_CG\_on\_paths|$  do
19:     $path\_combinations \leftarrow \text{combination}(valid\_CG\_on\_paths, m)$ 
20:    for all  $chosen\_groups \in path\_combinations$  do
21:      if  $\bigcap_{(P, groups) \in chosen\_groups} groups = \emptyset$  then
22:        return  $\text{get\_paths}(chosen\_groups)$ 
23:      end if
24:    end for
25:  end for
26: end if
27: return  $\text{no\_solution}$ 
```

A fractional relaxation over path weights $x_P \in [0, 1]$ yields a convex subproblem; we then round to k disjoint paths and place shares via π .

8 Results and Discussion

We evaluate the proposed secure key-relaying scheme via Monte Carlo simulation on randomly generated QKD relay networks modeled as undirected graphs. Each network is represented as a connected graph $G = (V, E)$ generated using a Harary graph generator [39], which guarantees connectivity while allowing controlled variation in topology. For each trial, we generate a connected Harary graph $H(n, \kappa)$, where κ is the target minimum node degree. We consider sparse-to-moderately connected relay

deployments by setting $\kappa \in \{2, 3, 4\}$. For each κ , we generate $T = 100$ independent graph realizations (distinct random seeds), yielding a total of $3T = 300$ network instances. Since the number of simple s - t paths grows rapidly with n , we do not enumerate all simple paths. Instead, we construct a candidate path set $\mathcal{P}$ by sampling feasible s - t routes as described below. Let $s = 0$ and $t = n - 1$. For each graph instance, we compute up to $P_{\max} = 200$ candidate s - t paths using a diversity-oriented variant of shortest-path sampling: (i) we compute the shortest path (Dijkstra/BFS since edges are unweighted), (ii) we iteratively compute additional paths by perturbing edge/node penalties to discourage reuse of previously selected internal vertices, and (iii) we retain only simple paths and discard duplicates. This yields a candidate set $\mathcal{P}$ of size $|\mathcal{P}| \leq P_{\max}$ with substantial overlap reduction, enabling evaluation of node-/group-disjoint routing preferences at scale.

Each relay node $A \in V \setminus \{s, t\}$ is assigned a curiosity value $\text{Curiosity}(A) \in [0, 1]$, and each unordered pair of relays (A, B) is assigned a symmetric collaboration value $\text{Collab}(A, B) = \text{Collab}(B, A) \in [0, 1]$. In the probabilistic model, we control the mean curiosity μ_c and mean collaboration μ_ℓ , and introduce heterogeneity around these means using bounded uniform sampling:

$$\text{Curiosity}(A) \sim \mathcal{U}(\max(0, \mu_c - \delta), \min(1, \mu_c + \delta)), \quad (14)$$

$$\text{Collab}(A, B) \sim \mathcal{U}(\max(0, \mu_\ell - \delta), \min(1, \mu_\ell + \delta)), \quad (15)$$

with $\delta = 0.1$. We sweep μ_c and μ_ℓ over $\{0.0, 0.1, \dots, 1.0\}$, yielding 11×11 behavior settings per topology. For each (μ_c, μ_ℓ) setting, we perform $R = 30$ independent behavioral assignments (different random seeds) and report results averaged over these R runs.

For deterministic experiments, curiosity and collaboration are binary ($\{0, 1\}$), forming collaborating groups as in Section VI-A. In this case, we prioritize *node-disjoint* and *group-disjoint* paths when constructing candidate path sets, and report feasibility and achieved Q under these constraints. For probabilistic experiments, curiosity and collaboration are continuous, and we report how m^* and Q^* vary with μ_c and μ_ℓ .

For each (n, κ) topology family, and for each (μ_c, μ_ℓ) behavioral setting, we report: (i) the optimal share count m^* , (ii) the minimized aggregated breaking probability Q^* , and where applicable, (iii) reliability trends using the surrogate in (16). All results are averaged over T graph realizations and R behavioral seeds, and we also report standard deviations to capture variability induced by topology and behavior heterogeneity.

The combined effect of curiosity and collaboration on the number of shares is shown in Fig. 1. At low collaboration levels, the number of shares required is maximum and sharply declines as the collaboration increases. As curiosity increases, the number of shares required remains unchanged except at low collaboration levels. These behaviors are discussed below.

Fig. 2 shows the effect of collaboration on the optimal key shares required. As the mean collaboration level of a network increases, the number of shares needed decreases. Since the goal is to minimise Q (as per (12)) for any given (fixed) curiosity level, the only parameter to minimise is the gathering probability, $\mathcal{G}_A$ (as per (6)). At

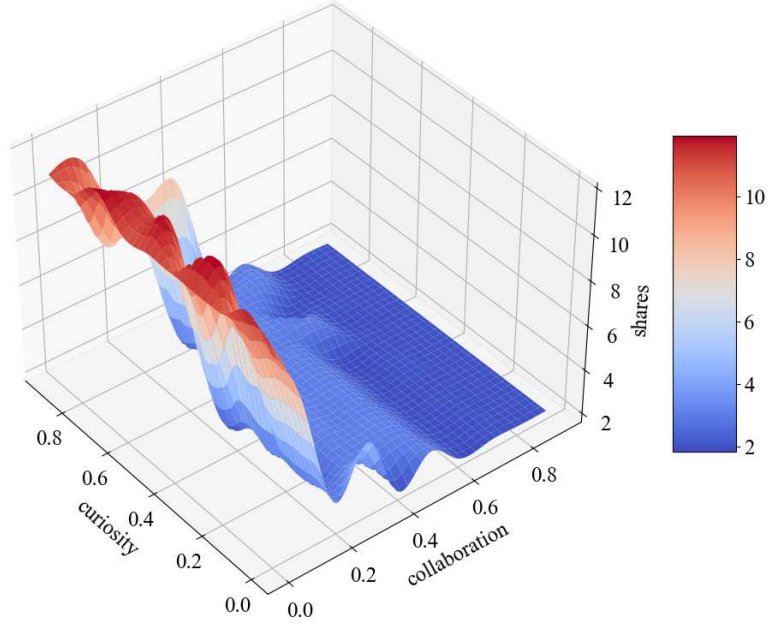


Fig. 1 Combined Effect on Optimal Shares

low levels of collaboration, selecting node-disjoint paths offers a benefit, resulting in an evenly distributed gathering probability. As collaboration in the network increases, breaking the key into more shares means that collaborating nodes can quickly gather the shares. Hence, we see a significant decline in the shares needed, typically saturating at a minimum of 2. Note that the anomalous behavior at extremely low curiosity levels ($0.0 - 0.1$) is due to the graph structure and does not correlate with curiosity. One-way ANOVA, Kruskal-Wallis H-test, and the Alexander-Govern test [40] yield that collaboration is independent of curiosity at $\alpha = 0.05$.

Mean curiosity levels, on the other hand, show a different behavior, as seen in Fig. 3. At moderate to high collaboration levels, the optimal number of shares decreases and saturates at two as the network's curiosity level increases. In this case, at a low curiosity level, since the relay nodes are more likely to collaborate, there is no benefit in increasing the number of shares, as seen by a lower peak. As curiosity rises, with an overall higher collaboration level, the breaking probability increases for larger m . Here, breaking the key into more shares has diminishing returns, so the number of optimal shares stabilises at two. This is not the case for low collaboration levels. At low collaboration levels, even at high curiosity levels, the breaking probability is minimised by opting for more shares. To mitigate the effect of higher curiosity, the algorithm opts for increased shares to decrease the gathering probability (see (6)) to decrease the breaking probability. Even as the curiosity increases, the gathering probability can be minimised only by having more shares. Furthermore, we can infer that curiosity is independent of collaboration at moderate to high levels of collaboration. However, it shows some correlation at lower levels of collaboration. Kruskal-Wallis H-test and the

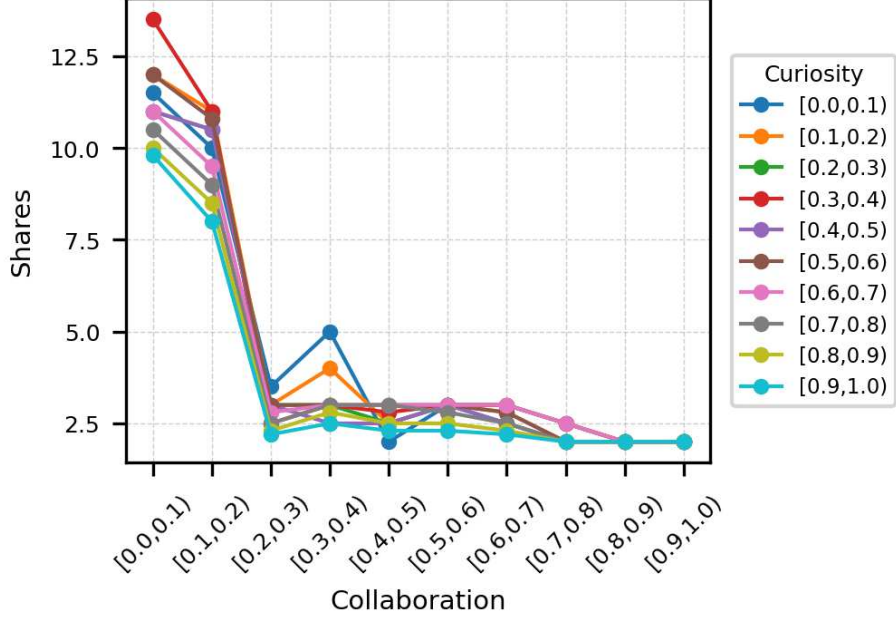


Fig. 2 Effect of Collaboration on Optimal Shares

Alexander Govern test indicate that curiosity is not independent of collaboration at $\alpha = 0.05$.

Fig. 4 and 5 show the effect of collaboration and curiosity on the breaking probability, respectively. From the graphs (fig. 4 and 5), (6), and (9), we know that as the collaboration or curiosity levels increase, the corresponding probabilities, $\mathcal{G}_A$ and Q_A also increase rapidly. More importantly, at high collaboration levels, $\mathcal{G}_A$ tends to maximise even at fewer shares. This is observed by the uniform behavior of both characteristics concerning the breaking probability.

Reliability Surrogate

Assuming independent compromise of share i with probability $\theta_i(p)$ along its path (affine in the malicious fraction p to first order), a tractable surrogate is

$$R(p) \approx 1 - \sum_{j=k}^m \sum_{\substack{S \subseteq S: i \in S \\ |S|=j}} \prod \theta_i(p) \prod_{i \notin S} (1 - \theta_i(p)). \quad (16)$$

The initial slope at $p = 0$ characterizes sensitivity and explains the observed diminishing returns with larger m .

Reliability degrades as the malicious-relay fraction increases (Fig. 6). Group-disjoint routing outperforms node-disjoint at the same shares m , and larger m improves

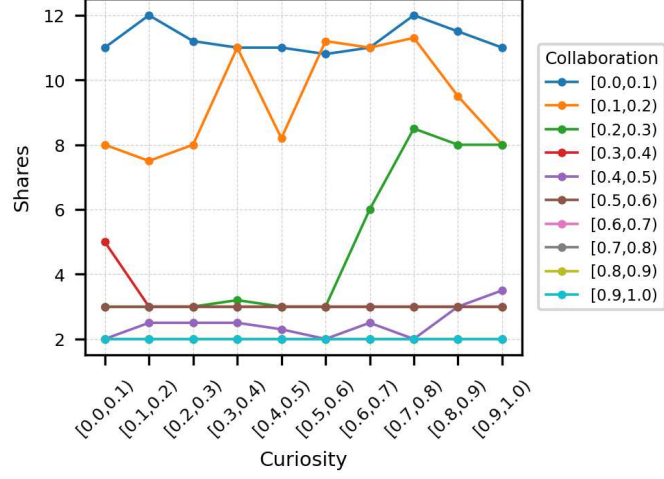


Fig. 3 Effect of Curiosity on Optimal Shares

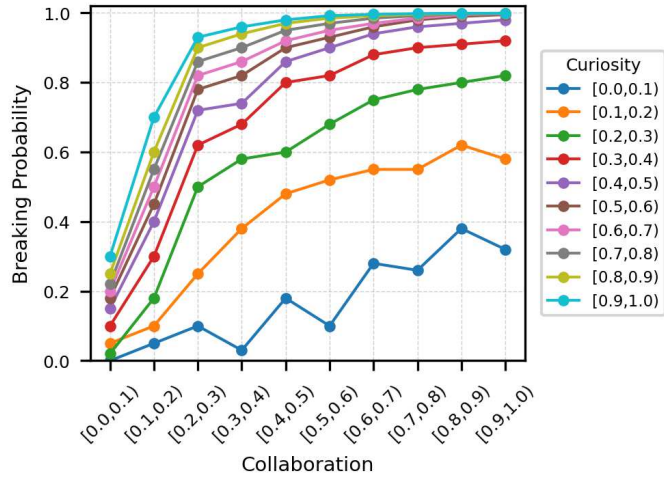


Fig. 4 Effect of Collaboration on Breaking Probability

resilience with diminishing returns. The CF variant (dashed) adds a modest gain at moderate adversary levels.

9 Conclusions and Future Works

QKD networks offer a fundamentally secure means of communication by leveraging the principles of quantum mechanics. However, malicious relay agents capable of compromising the secure key relaying process pose a challenge to the integrity of such networks. The existing methods primarily focus on extending the physical reach of

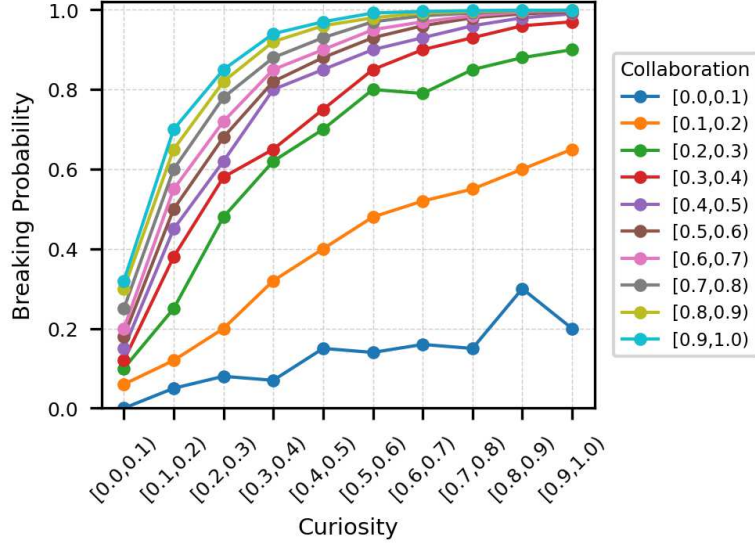


Fig. 5 Effect of Curiosity on Breaking Probability

QKD systems instead of mitigating threats caused by malicious nodes in the QKD network. Our paper introduces a novel application of Shamir’s secret-sharing to quantum communications, specifically tailored to fortify QKD networks against the risk posed by malicious intermediaries. By segmenting the quantum key into multiple shares and employing adaptive routing algorithms that dynamically adjust paths based on real-time threat assessments, our approach minimises the exposure of keys to potential interceptors. The probabilistic model effectively mitigates the risks posed by relay nodes with varying degrees of curiosity and collaboration, substantially lowering the likelihood of successful key compromises. In the future, more complex probabilistic modelling of relay trustworthiness can be considered, with specific attacks assigned their own probabilistic models.

The current algorithm employs a brute force approach, whereas a greedy, heuristic-based approach may yield suboptimal solutions that converge quickly. Another aspect to explore is the behavioral prediction of relay nodes using machine learning techniques, enabling even more dynamic and responsive security measures. Additionally, the scalability of the proposed methods could be tested in larger, more complex network environments to evaluate performance under diverse operational conditions. On the other hand, the result given in [41] works only for the deterministic model, since the study in [41] is based on a node being malicious or not, not on a probability of whether a node is malicious or not. Extending [41] to include this would be very interesting. Finally, extending our model to incorporate real-time data analysis could enhance the predictive capabilities, offering a more granular understanding of network security dynamics and automating the adjustment of security protocols in response to detected threats. This work focuses primarily on the optimality of segmenting the key into multiple shares in the presence of probabilistically malicious nodes, rather than

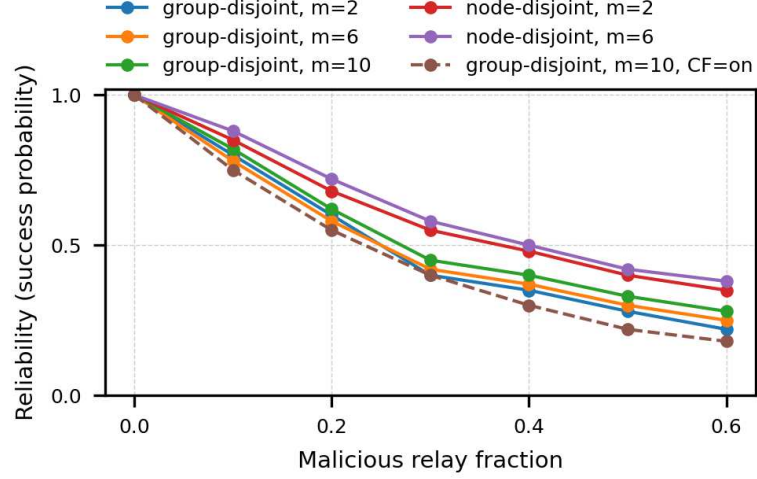


Fig. 6 Reliability vs. malicious-relay fraction for node- and group-disjoint routing at $m \in \{2, 6, 10\}$ (dashed: CF at $m = 10$). Larger m and group-disjoint routing yield higher reliability; gains taper at high m .

on modelling the curiosity and collaboration levels of the nodes. Also, we have only considered networks where adversaries do not modify the messages. However, we need a mechanism to detect these modifications or drops whenever nodes modify or drop messages.

Funding Declaration

No funding was received for this study.

References

- [1] Brazaola-Vicario, A., Ruiz, A., Lage, O., Jacob, E., Astorga, J.: Quantum key distribution: a survey on current vulnerability trends and potential implementation risks. *Optics Continuum* **3**(8), 1438–1460 (2024)
- [2] Zapatero, V., Curty, M.: Secure quantum key distribution with a subset of malicious devices. *npj Quantum Information* **7**(1), 26 (2021)
- [3] Lo, H.-K., Curty, M., Tamaki, K.: Secure quantum key distribution. *Nature Photonics* **8**(8), 595–604 (2014)
- [4] Ye, P., Chen, W., Zhang, G.-W., Lu, F.-Y., Wang, F.-X., Huang, G.-Z., Wang, S., He, D.-Y., Yin, Z.-Q., Guo, G.-C., *et al.*: Induced-photorefractive attack against quantum key distribution. *Physical Review Applied* **19**(5), 054052 (2023)

- [5] Jain, S., Jain, M., Kandwal, H.: Advanced algorithm for detection and prevention of cooperative black and gray hole attacks in mobile ad hoc networks. *International journal of computer Applications* **1**(7), 37–42 (2010)
- [6] Chen, H.-Z., Li, M.-H., Wang, Y.Z., Zhao, Z.-G., Ye, C., Li, F.L., Chen, Z., Han, S.-L., Tang, B., Miao, Y.J., Qi, W., *et al.*: Implementation of carrier-grade quantum communication networks over 10000 km. *npj Quantum Information* **11**, 137 (2025) <https://doi.org/10.1038/s41534-025-01089-8> . Open access
- [7] Kong, P.-Y.: Challenges of routing in quantum key distribution networks with trusted nodes for key relaying. *IEEE Communications Magazine* **62**(7), 124–130 (2024) <https://doi.org/10.1109/MCOM.023.2300376>
- [8] Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science* **560**, 7–11 (2014) <https://doi.org/10.1016/j.tcs.2014.05.025> . Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84
- [9] Yuan, Z., Dynes, J.F., Shields, A.J.: Avoiding the blinding attack in qkd. *Nature Photonics* **4**(12), 800–801 (2010)
- [10] Pirandola, S., Andersen, U.L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., *et al.*: Advances in quantum cryptography. *Advances in Optics and Photonics* **12**(4), 1012–1236 (2020)
- [11] Takeoka, M., Guha, S., Wilde, M.M.: Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature Communications* **5**, 5235 (2014)
- [12] Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. *Reviews of Modern Physics* **74**(1), 145–195 (2002)
- [13] Pirandola, S., Laurenza, R., Ottaviani, C., Banchi, L.: Fundamental limits of repeaterless quantum communications. *Nature Communications* **8**, 15043 (2017)
- [14] Phoenix, S.J.D., Barnett, S.M.: Relay QKD Networks & Bit Transport (2015). <https://arxiv.org/abs/1502.06319>
- [15] Elliott, C.: Building the quantum network. *New Journal of Physics* **4**, 46 (2002)
- [16] Briegel, H.-J., Dür, W., Cirac, J.I., Zoller, P.: Quantum repeaters: The role of imperfect local operations in quantum communication. *Physical Review Letters* **81**(26), 5932–5935 (1998)
- [17] Duan, L., Lukin, M.D., Cirac, J.I., Zoller, P.: Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414**, 413–418 (2001)
- [18] Elliott, C., Colvin, A., Pearson, D., *et al.*: Current status of the darpa quantum

- network. *Proceedings of SPIE* **5815**, 138–149 (2005)
- [19] Salvail, L., Peev, M., Diamanti, E., *et al.*: Security of trusted repeater quantum key distribution networks. *Journal of the Optical Society of America B* **24**(2), 398–409 (2007)
 - [20] Krawec, W.O.: Security of quantum key distribution with trusted nodes. *Quantum Information Processing* **17**(7), 1–17 (2018)
 - [21] Chen, Y.-A., Zhang, Q., Chen, T.-Y., *et al.*: An overview of quantum communication networks. *IEEE Communications Surveys & Tutorials* **23**(4), 1836–1861 (2021)
 - [22] Selentis, A., Makris, N., Papageorgopoulos, A., Konteli, P., Christodoulopoulos, K., Kanellos, G.T., Syvridis, D.: Evaluating Relayed and Switched Quantum Key Distribution (QKD) Network Architectures (2025)
 - [23] Shamir, A.: How to share a secret. *Commun. ACM* **22**(11), 612–613 (1979) <https://doi.org/10.1145/359168.359176>
 - [24] Fujiwara, M., Waseda, A., Nojima, R., Moriai, S., Ogata, W., Sasaki, M.: Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing. *Scientific Reports* **6**(1), 28988 (2016) <https://doi.org/10.1038/srep28988>
 - [25] Kong, P.-Y.: Challenges of routing in quantum key distribution networks with trusted nodes for key relaying. *IEEE Communications Magazine* **62**(7), 124–130 (2024) <https://doi.org/10.1109/MCOM.023.2300376>
 - [26] Quoc, C., Bellot, P., Demaille, A.: Stochastic routing in large grid-shaped quantum networks. In: 2007 IEEE International Conference on Research, Innovation and Vision for the Future, pp. 166–174 (2007). <https://doi.org/10.1109/RIVF.2007.369152>
 - [27] Liu, C., Che, X., Xie, J., Dong, Y.: A multi-path qkd algorithm with multiple segments. *Journal of Cyber Security and Mobility* **13**, 193–214 (2024) <https://doi.org/10.13052/jcsm2245-1439.1321>
 - [28] Wenning, M., Patri, S.K., Müller, J., Autenrieth, A., Elbers, J.-P., Rydlichowski, P., Mas-Machuca, C.: Towards optimized demand routing in qkd networks. In: 2023 Optical Fiber Communications Conference and Exhibition (OFC), pp. 1–3 (2023). <https://doi.org/10.1364/OFC.2023.Th2A.37>
 - [29] Hao, Y., Xie, Y., Gao, W., Tang, J.: Q-learning for resource-aware and adaptive routing in trusted-relay qkd network. *Photonics* **12**(10), 969 (2025) <https://doi.org/10.3390/photonics12100969>

- [30] Wang, J., Liu, X.-t.: Cascading attack on trusted-relay quantum key distribution networks. *Communications in Theoretical Physics* **73**(6), 065105 (2021) <https://doi.org/10.1088/1572-9494/abeedc>
- [31] Shafie, A.E., Sultan, A., Mabrouk, A., Tourki, K., Al-Dhahir, N.: Secret-key-aided scheme for securing untrusted df relaying networks. *IEEE Transactions on Vehicular Technology* **67**(7), 6727–6731 (2018)
- [32] Grillo, M., Dowhuszko, A.A., Khalighi, M.A., Hämäläinen, J.: Resource allocation in a quantum key distribution network with leo and geo trusted-repeaters. 2021 17th International Symposium on Wireless Communication Systems (ISWCS), 1–6 (2021)
- [33] Cao, Y., Zhao, Y., Li, J., Lin, R., Zhang, J., Chen, J.: Hybrid trusted/untrusted relay-based quantum key distribution over optical backbone networks. *IEEE Journal on Selected Areas in Communications* **39**(9), 2701–2718 (2021) <https://doi.org/10.1109/JSAC.2021.3064662>
- [34] Zhao, Y., Zhang, K., Zhu, Q., Wang, H., Yu, X., Zhang, J.: Applications of machine learning in quantum key distribution networks. In: 2021 IEEE 6th Optoelectronics Global Conference (OGC), Shenzhen, China, pp. 227–229 (2021). <https://doi.org/10.1109/OGC52961.2021.9654412>
- [35] Kong, P.-Y.: Routing with minimum activated trusted nodes in quantum key distribution networks for secure communications. *IEEE Internet of Things Journal* **11**(9), 15219–15228 (2024) <https://doi.org/10.1109/JIOT.2024.3349476>
- [36] Chen, L.-Q., Chen, J.-Q., Chen, Q.-Y., Zhao, Y.-L.: A quantum key distribution routing scheme for hybrid-trusted qkd network system. *Quantum Information Processing* **22**, 75 (2023)
- [37] Wang, J., Huberman, B.A.: A Reconfigurable Relay for Polarization Encoded QKD Networks (2021). <https://arxiv.org/abs/2106.01475>
- [38] Rani, P., Verma, S., Nguyen, G.N., *et al.*: Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network. *IEEE access* **8**, 121755–121764 (2020)
- [39] Harary, F.: The maximum connectivity of a graph $\sup_i \zeta_i^*/\sup_i \zeta_i$. *Proceedings of the National Academy of Sciences* **48**(7), 1142–1146 (1962) <https://doi.org/10.1073/pnas.48.7.1142> <https://www.pnas.org/doi/pdf/10.1073/pnas.48.7.1142>
- [40] Alexander, R.A., Govern, D.M.: A new and simpler approximation for anova under variance heterogeneity. *Journal of Educational Statistics* **19**(2), 91–101 (1994). Accessed 2024-11-12
- [41] He, X., Yener, A.: Cooperation with an untrusted relay: A secrecy perspective.

IEEE Transactions on Information Theory **56**(8), 3807–3827 (2010)