

Relayed vs. Switched QKD: A Comparison in Non-Uniform Ring Networks

Antonios Selentis-Boulntadakis
Department of Informatics and
Telecommunications
University of Athens
Athens, Greece
aselentis@di.uoa.gr

Konstantinos Christodouloupoulos
Department of Informatics and
Telecommunications
University of Athens
Athens, Greece
kchristodou@di.uoa.gr

George T. Kanellos
Department of Informatics and
Telecommunications
University of Athens
Athens, Greece
gtkanellos@di.uoa.gr

Abstract— The rise of quantum computers threatens public key security and its essential role in distributing symmetric keys. QKD offers a promising solution by leveraging quantum principles for secure key distribution between two points. To enable network-wide key distribution, two candidate architectures have emerged: Relayed QKD which relays neighboring generated keys along a path, and Switched QKD which uses optical switches to dynamically connect QKD devices and create key generation sessions between nodes. Both architectures require algorithmic solutions for effective key management and distribution. In prior work, we derived for uniform ring topologies optimal configurations and analytical formulas for keys consumption and compared the Switched and Relayed architectures. In this study, we extend that work by introducing scheduling and key management algorithms for arbitrary topologies and use them to compare these two architectures in non-uniform rings. Our findings reinforce previous conclusions: Switched QKD is more effective for dense (large number of nodes and short distances) networks, such as metropolitan rings, while Relayed QKD outperforms in larger rings with longer distances.

Keywords—Quantum Key Distribution, Secret Key Rate, key relays, multi-commodity flows, optical switches, scheduling, uniform and non-uniform rings, maximize key consumption rate

I. INTRODUCTION

In recent years, quantum computing has posed a security threat as new algorithms can use its power to break traditional network security practices relying on public key cryptography, such as the distribution of symmetric keys [1]. To address this, significant research and development has focused on Post Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). QKD is a promising solution for the distribution of keys that can be used for secure communication in the quantum era. Two key QKD architectures have emerged: Relayed QKD, where intermediate nodes relay keys as trusted entities across a path, and Switched QKD, which uses optical switches to dynamically establish QKD links between end-nodes.

In Relayed QKD the quantum fiber network can be a mesh. In such a quantum network, adjacent network nodes use an Alice-Bob pair while non-adjacent nodes secure their communication by relaying keys through intermediate nodes [1] at the KMS level (Fig. 1a). Typically, in QKD networks, each node is equipped with a Key Management System (KMS) server, where keys are managed and buffered. In Relayed QKD the KMS plays the important role of relaying the keys. To achieve the highest security, one time pad (OTP) is used, where the KMS server of an intermediate node uses two keys - one from the previous QKD link and one from the next on the specific path. In Relayed QKD the number of

quantum pairs is kept low, equal to the number of quantum network fiber links. So, in a typical mesh quantum network with $O(N)$ fibers, only $O(N)$ QKD device pairs are needed. However, to secure all-to-all connections, each node participates in $O(N^2)$ key relaying paths, and, as so, the keys are split among numerous relays. The decision of relay paths and the split of keys among them requires a multi-commodity flow algorithm to perform it efficiently.

In Switched QKD each network node is equipped with quantum devices (one Alice and one Bob in our comparison), which are connected to a low-loss optical switch, which, in turn, is connected to all other nodes requiring secure communication with fibers. Assuming that any Alice can establish a QKD link with any Bob, optical switches enable dynamic QKD link establishment (referred also as key generation session) by connecting an Alice/Bob to a Bob/Alice at another node. The QKD connections/links can be implemented using: (i) the same fiber in the quantum layer, with (i.a) different wavelengths for simultaneous quantum key generation sessions, or (i.b) the same wavelength while avoiding simultaneous key sessions on the quantum layer fiber paths; or (ii) dedicated fibers in the quantum layer, between nodes requiring secure communication. In this paper, we consider option (ii), since fibers are typically abundant; the performance results were quite similar for option (i.a). In a network with N nodes requiring secure communication between each pair, this architecture requires N device pairs (Fig. 1b) as opposed to $(N^2-1)/2$ pairs required without switching. However, since QKD devices are limited, they cannot generate keys for all pairs simultaneously. Instead, a QKD link, is established between two nodes for limited time, after which is released and the devices repurposed for other QKD links. In Switched QKD, each module's KMS server stores keys during an active QKD link session and uses them even when the QKD link is inactive. To ensure availability, the KMS buffers of each node should be replenished by properly configuring the related QKD links. Also, note that longer-distance/higher-attenuation QKD links generate keys at a lower rate, and thus require more active QKD link time to replenish their buffers. These issues necessitate a scheduling algorithm to efficiently manage the QKD link sessions.

To evaluate the Relayed and Switched QKD architectures, we derived for uniform ring networks optimal configurations and analytical formulas, and used those to compare their efficiency [3]. Our results showed that Switched QKD performs better in uniform rings with short distances and many nodes, while Relayed QKD outperforms in the opposite scenarios. In this work we extend the comparison to more

realistic non-uniform rings. To perform this comparison, we made targeted modifications to two integer linear programming (ILP) formulations that each solve the related optimization problem (dynamic scheduling of QKD links/sessions in Switched QKD [4], and dividing the keys among relay paths in Relayed QKD [5]). Our modifications ensured directly comparable outputs and lower running times. We reached similar conclusions for non-uniform rings. Specifically, Switched QKD continues to perform best in networks with shorter average node distances—up to 7.5 km for networks with up to 13 nodes, and up to 5 km for larger networks of up to 21 nodes. When average node distances exceed 15 km in sparse networks and 10 km in more dense networks, Relayed QKD outperforms Switched QKD.

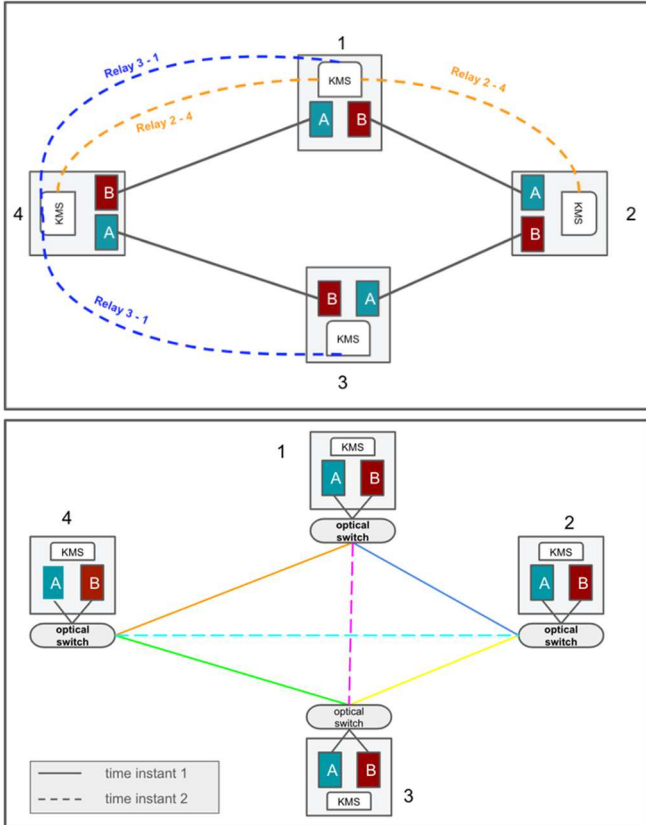


Figure 1 Example of: a) Relayed and b) Switched QKD networks of 4 nodes.

II. RELATED WORK AND CONTRIBUTIONS

The majority of the research in QKD has focused on the physical layer, the creation of the QKD link and of protocols to create keys at the two endpoints. However, a QKD link is inherently point-to-point and thus providing network-wide security requires some advanced network architecture. In this direction, in recent years, both Relayed and Switched QKD network architectures have been actively studied; these architectures introduce key management and orchestration problems, which are combinatorial optimization problems: managing of the key relays and scheduling of the QKD sessions, respectively.

The Relayed QKD is considered a mature architecture, and several algorithms have been proposed to solve the related key management optimization problem. [6] proposed five algorithms and conducted a comparative analysis, concluding that ILP formulations, while having the highest

computational requirements, achieve the best performance. [7] and [5] proposed ILP models to optimize multi-commodity key relays as well as heuristics. The maturity of the Relayed QKD architecture has led to relevant KMS implementations, e.g. by evolutionQ and IDQ Clarion which include key relay optimization algorithms [8][9][10]. In this study we chose to extend the algorithm proposed in [5], as it was the most easily adaptable and allowed for a direct comparison between the two architectures.

The Switched QKD architecture, although still experimental, has been demonstrated in several setups. Notably, [11] demonstrated a four-node network free of trusted nodes, showcasing, thus, the practical viability of the Switched architecture. At the same time, the Switched architecture has gained initial support from the QKD industry [12]. The orchestration in such architecture involves the complex scheduling of QKD sessions between nodes, that is, the dynamic creation and release of QKD links. The authors of [13] proposed a joint approach that combines the Relayed QKD architecture with a variant of Switch QKD, where optical switches bypass intermediate nodes. The study introduced two heuristic algorithms: for a network with full and with limited bypass-capabilities. Paper [14] investigated the complexity of the switched QKD scheduling problem and presented a proof of its NP-hardness. Additionally, [14] proposed an ILP model that establishes QKD links to maximize key requests served within a given period, assuming no reconfiguration of QKD links during that. In the subsequent period, the QKD links are reconfigured to address previously unaccomplished requests, and the process repeats. Furthermore, [14] presented a heuristic algorithm offering fast yet suboptimal solutions.

In contrast, in [4], we proposed an algorithm for a single scheduling period, calculating a global schedule that maximizes the minimum key consumption rate by allowing QKD links to be reconfigured at selected time instances within the period. In a real-world scenario the algorithm could recompute the global schedule with updated inputs (i.e. Secret Key Generation Rates - SKGR) before the start of each period. In [3] we derived optimal configurations and formulas for the Switched and Relayed QKD in uniform rings, where adjacent nodes have equal SKGR. We then compared their performance across different ring sizes and node distances. In this work, we extend [4] and [5] to develop algorithms that optimize Switched and Relayed architectures for generic topologies, focusing on improving their running times and aligning their outputs for a consistent comparison. Using these we present a comparison of Switched and Relayed QKD in non-uniform rings.

III. NETWORK MODELING

We discuss here the Switched QKD and Relayed QKD architectures, outline the optimization problems and (I)LP models to solve those. For Switched QKD, we start with an ILP model which is generic and can handle any topology and then extend it, adding constraints to reduce the solution space and its execution time in ring networks. For the Relayed QKD we discuss an LP model, which extends [5], which can efficiently optimize generic and ring topologies. The Switched QKD problem definition and ILP formulation introduce certain novelties, so we present them in more detail.

We assume a typical QKD control architecture consisting of 3-layers. The quantum layer, as the first layer, consists of quantum devices (Alices and Bobs) that are connected over dedicated fibers (the quantum network). The second layer is the key management system (KMS), where each node hosts a KMS server. These servers handle the quantum device-generated keys, by storing them in buffers. In case of the Relayed QKD the KMS servers transfer keys encrypted over the regular data network to other KMS servers. Thus, the KMS plays a slightly different role in the two QKD architectures. In the third layer, secured application entities (SAEs) use the symmetric keys stored in the KMS servers' buffers to encrypt, e.g. with AES, their communication over the regular data network. We will assume an all-to-all consumption profile: at each node we have one SAE communicating with another SAE in each other node, but the models can be easily extended for other consumption profiles. We will also assume that we maximize the minimum consumption rate across all SAE pairs, so as to ensure fairness in security. The KMS oversees the entire process and maintains distinct buffers for each pair of SAEs. Note that we use the term *generation* to refer to the QKD devices communication, which represents the output of the QKD/quantum network to the KMS servers. Conversely, we use *consumption* to denote the use of keys by communicating SAEs, that is the output of the KMS servers to the SAEs.

A. Switched QKD Network

In the Switched QKD architecture, each node i is equipped with a number of quantum devices. For our simulations, we used one Alice and one Bob, but we define the problem in a more generic way here. For a node i , we denote by I^A the number of Alice and I^B the number of Bob devices. These devices are connected to a low-loss optical switch, enabling the dynamic establishment of QKD links between an Alice at node i (from I^A) and a Bob at j (from J^B) or the opposite. We assume that we have dedicated fiber links for the quantum layer between any two nodes, for the all-to-all node consumption scenario. While a QKD link between nodes (i,j) is active, keys are generated at a secret key generation rate (SKGR) G_{ij} which is assumed to be known (averaged over previous timeslots, modeled, or predicted), which can also account for the specific devices. For our simulations, we used a SKGR function of attenuation fitted from measurements of Toshiba QKD devices [15]. Note that the SKGR depends on the attenuation which depends on distance, and is, in fact, inversely proportional to those.

We assume that the network operates in periods of length T , where at the start of a period we know the average SKGR G_{ij} (e.g. observed in the previous period, in our simulations modeled as a function of distance). The QKD link (i,j) is established for duration d_{ij} in the period T and the keys are stored at buffers at i 's and j 's KMS servers. These keys are continuously consumed (by SAEs) at a constant consumption rate c_{ij} , both during the time the QKD link is active and afterward. Thus, the keys generated in d_{ij} must be greater or equal to the keys consumed in the whole period: $d_{ij}G_{ij} \geq Tc_{ij}$. The related KMS buffers have limited capacity M_{ij} , dropping the excess keys. To simplify the problem and notation, we assume equal buffers M for all pairs. The KMS buffer size M limits the maximum consumption rate: $c_{ij}(T - d_{ij}) \leq M$. QKD devices are used once at any time, with a reconfiguration time

R for switching QKD links and an extra attenuation penalty P due to the optical switches. This extra penalty P can also account for SKGR performance penalties due to the non-matching of QKD devices (an Alice talking to different Bobs and vice versa). Fig. 2 shows a sample schedule for the network depicted in Fig. 1b and evolution of the key levels. In practice, the SKGR varies over time and it may differ from the one used as input. Then the keys remaining in the buffers at the end of the period could deviate from those calculated. In such case, the scheduling algorithm should be re-executed, taking into account the updated SKGR, to (re)calculate the schedule for the next period. Moreover, based on the variability of the averaged SKGR we can define a key margin to target by the end of the period, ensuring that keys are not depleted despite the varying SKGR.

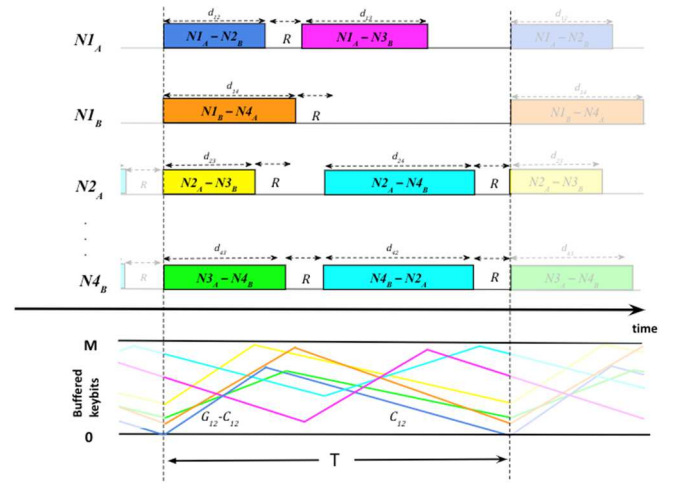


Figure 2: Schedule sample of QKD links (key generation sessions) and corresponding level of key buffers for the network of 4 nodes shown in Fig. 1.b (colors code the QKD links) for a period T .

As is evident, a scheduling algorithm is necessary to efficiently allocate the key generation sessions / the QKD links establishments and releases / between the nodes within the period T . The objective we consider is to maximize the minimum key consumption rate, that is, $\max: \min_i(c_{ij})$.

1. Switched QKD- ILP model for arbitrary networks

While in [3] we constructed optical schedules that maximize the minimum consumption rate for uniform rings, real-world networks are heterogeneous. Therefore, in [4], we proposed an optimal scheduling algorithm based on ILP for arbitrary topologies and given SKGR. The ILP model presented in the following is an improved version of [4] where two constraints were combined to improve the running time. Extension of this generic ILP model for rings that reduce the solution space and substantially improve the running time is discussed in the following subsection.

We assume a Switched QKD network topology with N nodes, where each node i has I^A number of Alice and I^B number of Bob devices. We assume the presence of SAE pairs (i,j) requiring keys between all pairs of nodes that is for i and $j=1, \dots, N$. For each SAE pair (i,j) we assume one generation session (establishment and release of a QKD link) in the period T . The average SKGR, G_{ij} , between each nodes pair is known, accounting for link losses and impairments, optical switches and any penalty for the arbitrary communication of the QKD devices. We assume that keys are extracted from the

QKD devices and stored at a KMS server at each node, with separate buffers for each i, j , each of size M . We also assume a large integer $bigM \geq T$. The consumption rate of SAE pair (i, j) is denoted by c_{ij} . The objective is to maximize the minimum consumption rate c_s , $c_s \leq c_{ij}$, across all pairs. The algorithm calculates the periodic schedule consisting of starting times s_{ij} and durations d_{ij} of the QKD links / key generation sessions for all node pairs (e.g. Fig. 2).

The updated ILP scheduling model is as follows.

Variables:

- c_s : float, minimum consumption rate of Switched QKD
- c_{ij} : float, consumption rate of SAE pair (i, j)
- s_{ij} : float, start time of QKD link (i, j) configuration
- d_{ij} : float, duration of QKD link (i, j) configuration
- x_{ij} : binary, equal to 1 if Alice in i and Bob in j , or 0 if inverse
- e_{ijk} : binary, equal to 1 if the end time of QKD link (i, j) is before the start time of (i, k) , that is, if $s_{ij} + d_{ij} + R < s_{ik}$
- a_{ijk} : binary, equal to 0 if pair (i, j) and pair (i, k) both use Alice in i and overlap in time, else 1
- b_{ijk} : binary, equal to 0 if pair (i, j) and pair (i, k) both use Bob in i and overlap in time, else 1

ILP formulation:

max: c_s , subject to:

For all nodes i, j :

$$T \geq s_{ij} + d_{ij} + R$$

For all nodes i, j :

$$c_{ij} \cdot T \leq d_{ij} \cdot G_{ij}, c_s \leq c_{ij}$$

For all nodes i, j :

$$c_s \leq c_{ij}, c_{ij} \cdot (T - d_{ij}) \leq M$$

For all nodes i, j :

$$x_{ij} + x_{ji} = 1, s_{ij} = s_{ji}, d_{ij} = d_{ji}$$

For all nodes $i, j, k \neq j$:

$$s_{ik} - (s_{ij} + d_{ij} + R) \leq e_{ijk} \cdot bigM, s_{ik} - (s_{ij} + d_{ij} + R) \geq (e_{ijk} - 1) \cdot bigM$$

For all nodes $i, j, k \neq j$:

$$a_{ijk} \leq x_{ji} + x_{ki} + e_{ijk} + e_{ikj}, b_{ijk} \leq x_{ij} + x_{ik} + e_{ijk} + e_{ikj}$$

For all nodes i, j :

$$I^A \geq x_{ij} + \sum_{k \neq j} (1 - a_{ijk}), I^B \geq x_{ji} + \sum_{k \neq j} (1 - b_{ijk})$$

The objective for the Switched QKD architecture is to maximize the minimum consumption rate (c_s) across all node pairs, ensuring fairness in security. With such objective, the algorithm improves the lowest consumption rate by reallocating resources (time) from other pairs. As the worst consumption rate improves, the algorithm shifts focus to the next lowest. This continues until the consumption rates across the network are relatively balanced—or, more precisely, until no further improvements can be made to the worst without making another lower than that. C1 ensures that key generation sessions are bounded in time by the period. C2 ensures that the number of consumed keys does not exceed the number of keys generated within the period. C3 bounds the minimum consumption rate, and consumption rates according to the buffer size. C4, ensures symmetry, by enforcing that each Alice can establish a QKD link only with a Bob, and vice versa. C5 identifies the collisions of key generations sessions, that is, if sessions overlap in time, using BigM. Considering the possible relative positions of sessions (i, j) and (i, k) : either (1) (i, j) ends before (i, k) starts, or (2) (i, j)

ends after (i, k) starts. In case (1) the first equation of the constraint forces e_{ijk} to take the value 1, as $s_{ik} > (s_{ij} + d_{ij} + R)$. Conversely, in case (2), the second equation of the constraint forcing e_{ijk} to take the value 0, as $s_{ik} < (s_{ij} + d_{ij} + R)$. Similarly, e_{ikj} takes the value of 1 if (i, k) starts after the end of (i, j) , and 0 otherwise. Thus, these constraints sets both e_{ijk} and e_{ikj} to 0 if (i, j) and (i, k) overlap in time (so when (i, j) does not end before the start of (i, k) , and (i, k) does not end before the start of (i, j)). Consequently, C6 ensures that for pairs (i, j) and (i, k) , where node i uses Alice for generation ($x_{ij} = 1$ and thus $x_{ji} = 0$, $x_{ik} = 1$ and thus $x_{ki} = 0$), the variable a_{ijk} takes the value 0 when both $e_{ijk} = 0$ and $e_{ikj} = 0$. This means that a_{ijk} is equal to 0, only when key generation sessions of (i, j) and (i, k) use both Alice and overlap in time. Similarly, for Bob's usage, the variable b_{ijk} is constrained according to the same logic. C7 controls the assigned number of quantum devices per node. In our comparison, as mentioned earlier, we assumed one Alice and one Bob per node, so we set $I^A = 1$ and $I^B = 1$.

2. Switched QKD- ILP model for rings

The previous ILP model is applicable to any topology, and thus can also optimize schedules for uniform and non-uniform rings. After observing optimal solutions in rings, we derived the following constraints that reduce the solution space in rings, thus significantly decrease the run-time while still providing a high-quality solution:

$$C1 \quad \text{For all nodes } i (i=1, \dots, N) \text{ and } j (j=1, \dots, \frac{(N-1)}{2} - 1): \quad C7$$

$$C2 \quad x_{i, (i+j) \% N} = x_{(i-j) \% N, i}$$

$$C3 \quad \text{For all nodes } i (i=1, \dots, N) \text{ and } j (j=1, \dots, \frac{(N-1)}{2} - 1): \quad C8$$

$$s_{i, (i+j) \% N} \geq s_{i, (i+j+1) \% N}$$

C4 Specifically, C7 enforces that if node i establishes a QKD link with node $(i+j) \% N$ using Alice then it will use Bob to establish a QKD link with the symmetric node $(i-j) \% N$, or the opposite. The expectation is that these QKD links will have similar distances and will be scheduled roughly at the same time and thus they can use the two available (Alice and Bob) QKD devices at node i . Additionally, C8 provides a simple schedule ordering based on the hop-distance, so as to exclude multiple equivalent solutions with different time sequences and reduce the run-time.

B. Relayed QKD Network

In the Relayed QKD architecture we have a mesh quantum network and each quantum fiber link is equipped with an Alice-Bob pair at its ends, enabling the establishment of QKD links between adjacent nodes. For communication between distant nodes, keys are generated along one or more paths of direct QKD links, with intermediate nodes acting as trusted nodes at the KMS layer and relaying the keys from the source to the destination. The KMS server at the source transfers a key to the next hop KMS server on the path by encrypting it (XORed with a key of the specific QKD link – assuming one time pad). The next hop KMS server decrypts it and encrypts it with the next-link key and so on, ensuring that the source key securely reaches the destination. Thus, relaying keys for nodes (s, d) consume keys from all QKD links (i, j) along the path p_{sd} , while the end-to-end key consumption rate c_{sd} is the minimum of the contribution rates of all intermediate QKD links, $c_{sd} = \min_{i, j \in p_{sd}} c_{ij}^{sd}$. Direct QKD links can be considered as a single link path and thus are included in this concept. The

KMS orchestrator decides on the relay paths and key rate contributions c_{ij}^{sd} for each QKD link for all (s,d) pairs: $G_{ij} = \sum_{sd} c_{ij}^{sd}$. This is a variation of the multicommodity flow optimization, typical in graphs and networks.

For a uniform ring with equal attenuation and generation rates between adjacent nodes, an optimal key flow solution can be constructed [3]. For non-uniform networks, an ILP model to obtain the optimal solution assuming integer flows and optimizing a weighted combination of the average and minimum of number of keys generated was presented in [5]. For the purposes of this work we modified [5] model, i) to account for bidirectional demands, ii) changed the objective function to maximize the minimum consumption rate $c_R \leq c^{sd}$ for the Relayed QKD architecture, and iii) assumed floating variables (consumption rates) to formulate the problem as an LP that could be optimally solved in polynomial time.

IV. COMPARISON FOR NON-UNIFORM RING NETWORKS

We performed a comparison of the Relayed and Switched QKD network architectures in non-uniform ring networks. We assumed one Alice and one Bob quantum device at each node. For Switched QKD, we used the ILP formulation (Section V.A.1) augmented with the additional constraints for the reduction of runtime (Section V.A.2) to calculate the optimal schedule and the maximum minimum consumption rate c_s . Even so, for some scenarios in large rings, the optimal solution was not tracked within 2 hours and for those we used the best solution found up to that point. For the Relayed QKD architecture we used the algorithm presented in [5] with some minor modifications, discussed at the end of Section V.B, to calculate the maximum minimum consumption rate c_R , for the same inputs, ensuring thus a fair comparison. We compared the solutions for various non-uniform ring scenarios, considering different number of nodes, average adjacent QKD link lengths, and length deviations.

We assumed ring topologies for the quantum layer, with fiber links between neighboring nodes and additional chord quantum fiber links in the Switched architecture. As mentioned in Sec. 1, we could also consider a Switched Network with the same links using different wavelengths, but the performance was quite similar. The secret key generation rate (SKRG) function g was modeled based on Toshiba's Quantum Devices [15]. For QKD link (i,j) the SKGR was defined in terms of the attenuation, as $G_{ij}=g(A_{ij})$, where the QKD link attenuation $A_{ij}=a_c D_{ij}$ was proportional to the distance D_{ij} , and a_c was the attenuation coefficient, which was set to 0.22 dB/km. In the Relayed architecture, we assumed only fiber links between ring adjacent nodes, so D_{ij} was defined only for adjacent nodes (i,j) and was equal to their distance, i.e. $D_{ij}=L_{ij}$. In the Switched architecture, we assumed chord quantum fiber links, so D_{ij} was the corresponding chord distance between any node pair (i,j) . For Switched, we also assumed a scheduling period, $T=180$ min, a reconfiguration time between key-generation sessions, $R=5$ min, and additional losses caused by the optical switches, $P=2$ dB. The quantum devices measured, similar to most network devices, are designed to operate within a receiver dynamic range of -5 dBm to -22 dBm, requiring additional attenuators when the received power approaches -5 dBm. Due to this, we considered a threshold (flat) distance of 20 km, below which the generation function does not increase.

To simulate non-uniform rings we considered an average adjacent node distance L and a distance deviation factor f and drew the distance of each quantum link from a uniform distribution, with a range of $(L-Lf, L+Lf)$. We simulated non-uniform rings with different numbers of nodes N ($=5,7,9,13,17,21$), different average adjacent node distance L ($=2.5, 5, 7.5, 10, 15, 20$ km) and distance deviation factor f ($=0.1$ and 0.5). For each network scenario (N, L and f), we generated 10 (non-uniform) ring instances, with random adjacent node distances drawn from the uniform distribution, and then solved the related ILP/LP model using CPLEX. For the Switched QKD and computationally complex scenarios with $N=17$ nodes or more, we stopped the simulation after 2 hours. To compare Switched QKDS's optimal consumption rate (c_s) and η_{KS} Relayed QKD's consumption rate (c_R) we introduced a *relative consumption performance* metric ρ as:

$$\rho = 100 \cdot (c_s - c_R) / \max(c_s - c_R),$$

whose values range from -100 (Relayed outperforms) to +100 (Switched outperforms). For each scenario we found the consumption rates, calculated the relative consumption ρ , and averaged ρ over 10 scenarios for each set of input parameters.

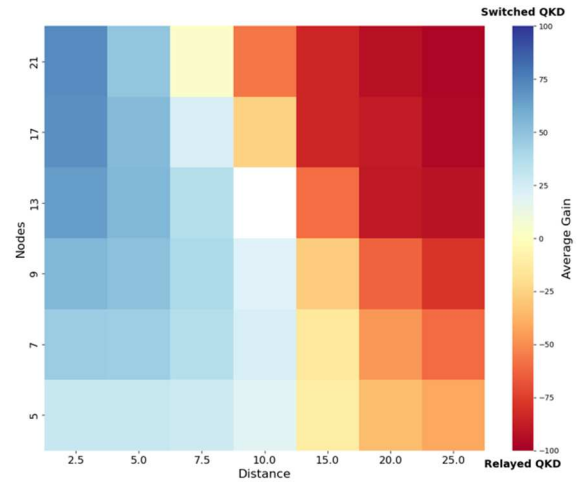


Figure 3: Average relative consumption rate for a distance deviation factor $f=0.1$, and various length distances L and number of nodes N .

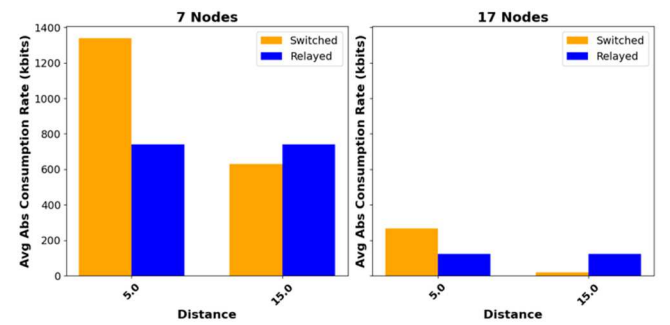


Figure 4: Average absolute key consumption rates for a length deviation factor $f=0.1$, distance $L=5$ and 15 km, and a) $N=7$ nodes, and b) $N=17$ nodes.

Fig. 3 shows the average relative performance for non-uniform ring networks and a deviation factor of $f=0.1$. The Switched QKD architecture demonstrates relatively superior performance in scenarios with short distances between nodes, as the previously mentioned flat key generation distance (constant key generation below 20 km) limits Relay's ability to increase its key rate for average distances $L \leq 20$ km. Specifically, we observe a high relative gain ($\rho > 25$) across

all network scenarios with $L \leq 7.5$ km for small networks ($N \leq 13$). For short distances ($L \leq 5$ km), we observe an even higher relative gain ($\rho > 50$) in networks with $N \geq 9$, which increases as networks become denser. For longer distances, $L \geq 20$ km for networks with $N \leq 7$ nodes, $L \geq 15$ km for $N=9$ and 13, and $L \geq 10$ km for $N \geq 17$, the Relay QKD architecture outperforms the Switched QKD architecture, achieving a relative gain of up to $\rho = 60$ in smaller networks and up to $\rho = 97$ in larger networks. The intermediate scenarios fall within a gray zone where neither architecture is significantly better; a specific network scenario would require to run both optimization algorithms to determine the best choice.

Fig. 4a and b present the absolute key consumption rates for non-uniform rings with $f=0.1$ and $N=7$ and $N=17$. Note that absolute rates depend highly on the specific SKGR model used (Toshiba QKD devices), whereas their relative comparison depends on the shape of the SKGR function and is more general. For $N=7$ and average distance $L=5$ km (and $f=0.1$) the Switched QKD architecture achieves an average absolute key consumption rate of 1340.5 kbits/sec, while the Relay architecture has an average absolute key consumption rate of 740.3 kbits/sec. Conversely, for average distance $L=15$ km, the Relay architecture outperforms the Switched QKD architecture with an average absolute key consumption rate of 740.3 kbits/sec compared to 631.5 kbits/sec. Similarly, for networks with $N=17$ nodes (Fig. 4b), the Switched QKD architecture exhibits significantly better relative performance for $L=5$ km, and rate of 266.5 kbits/sec compared to 123.4 kbits/sec). However, for longer average distances and in particular $L=15$ km, the Relayed QKD becomes the only realistic option, with a rate of 123.4 kbits/sec (low due to the flat distance), as the Switched architecture completely fails to function, since the maximum distance of the assumed QKD devices is shorter than the longest chord distance.

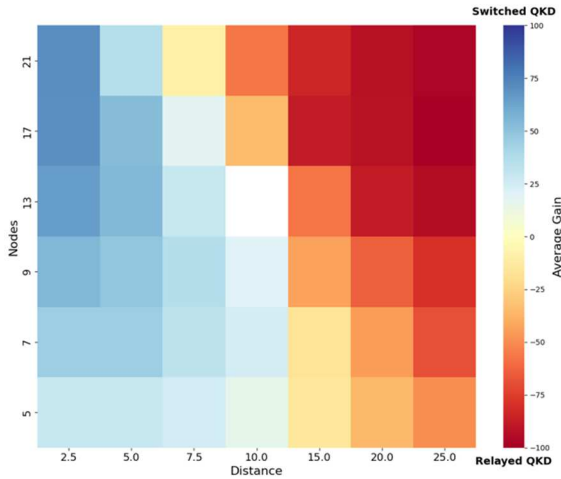


Figure 5 Average relative consumption rate for length deviation factor $f=0.5$ and various length distances L and number of nodes N .

Fig. 5 shows the relative performance for a length deviation factor $f=0.5$. The results were similar, with an improvement compared to $f=0.1$ in the relative performance of the Relayed architecture in scenarios with $L \leq 15$ km, as Switched QKD's performance was slightly reduced due to the network's increased heterogeneity. Switched QKD continues to outperform in dense rings while Relayed in larger networks. With $f=0.5$, the ring scenarios span a wide range, reflecting real-world networks. Thus, these results effectively illustrate

the relationship between Switched and Relayed performance across various average distances and network sizes.

V. CONCLUSION

To enable network-wide key distribution, both Relayed QKD and Switched QKD network architectures have been proposed and studied. Both architectures require algorithmic solutions for effective key management and distribution. We presented a novel ILP scheduling model for Switched QKD that maximizes the minimum consumption rate and two additional constraints that accelerate its execution by producing near-optimal solutions. Subsequently, we used this formulation to compare the performance of Switched QKD with that of Relayed QKD across various non-uniform ring network scenarios. The results reinforced our previous findings for uniform rings. In the more realistic non-uniform rings, Switched QKD is more effective for dense networks with short distances between nodes, such as Metropolitan Networks, while Relayed QKD outperforms in larger networks with longer distances, such as metro/core networks.

VI. ACKNOWLEDGEMENTS

This work was partially funded by HFRI project DetermIneD, under the call "Basic research Financing (Horizontal support of all Sciences)" under the National Recovery and Resilience Plan "Greece 2.0", funded by the E.U.

VII. REFERENCES

- [1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, 1994.
- [2] Chip Elliott, "Building the quantum network", 2002 New J. Phys. 4 46.
- [3] N. Makris et al., "Relayed-QKD and switched-QKD networks performance comparison considering physical layer QKD limitations," *Optical Fiber Communications Conference and Exhibition (OFC)*, San Diego, CA, USA, 2024.
- [4] K. Christodouloulopoulos, et al., "Optimizing Key Consumption in Switched QKD Networks," *Optical Fiber Communications Conference and Exhibition (OFC)*, San Diego, CA, USA, 2024.
- [5] C. Lee et al., "Key-count differential-based proactive key relay algorithm for scalable quantum-secured networking," in *Journal of Optical Communications and Networking*, vol. 15, no. 5, 2023.
- [6] T. Johann et al., "Comparison and optimization of different routing methods for meshed QKD networks using trusted nodes," in *Journal of Optical Communications and Networking*, vol. 16, no. 3, 2024.
- [7] Y. Cao, Y. Zhao, Y. Wu, X. Yu and J. Zhang, "Time-Scheduled Quantum Key Distribution (QKD) Over WDM Networks," in *Journal of Lightwave Technology*, vol. 36, no. 16, 2018.
- [8] G. Kanellos et al., "Advanced key management in switched QKD networks with non-optimized QKD links", Proc. SPIE PC12911, Quantum Computing, Communication, and Simulation IV, 2024.
- [9] www.idquantique.com/quantum-safe-security/products/clarion-kx-platform/
- [10] www.evolutionq.com/products/basejumpqdn
- [11] O. Alia et al., "Dynamic DV-QKD Networking in Trusted-Node-Free Software-Defined Optical Networks," in *Journal of Lightwave Technology*, vol. 40, no. 17, 2022.
- [12] www.thinkquantum.com/wp-content/uploads/files/Brochure_QUKY.pdf
- [13] K. Dong et al., "Auxiliary graph based routing, wavelength, and time-slot assignment in metro quantum optical networks with a novel node structure," *Opt. Express* 28, 2020.
- [14] Q. Zhang et al., "Routing, Channel, Key-Rate, and Time-Slot Assignment for QKD in Optical Networks," in *IEEE Transactions on Network and Service Management*, vol. 21, no. 1, 2024.
- [15] www.global.toshiba/ww/products-solutions/security-ict/qkd/products.html