

Comparing Relayed and Switched QKD in Ring Networks

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

Konstantinos Christodoulouopoulos
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 cryptography and its foundational role in secure symmetric key distribution. Quantum Key Distribution (QKD) offers a promising alternative, leveraging quantum principles to securely distribute keys between two endpoints. To enable network-wide key distribution, two main architectures have emerged: Relayed QKD, which forwards keys generated between neighbors along a path, and Switched QKD, which uses optical switches to dynamically establish QKD links between nodes for scheduled key generation sessions. Both architectures require algorithmic solutions for efficient key management and distribution. We present optimal configurations and analytical formulas for uniform rings and compare the performance of the two architectures. We also define generic key management algorithms and apply them to compare the two architectures in non-uniform rings. Our findings are consistent across both uniform and non-uniform rings: Switched QKD is more effective in dense networks (i.e., with many nodes and short distances), while Relayed QKD performs better in larger rings with longer inter-node distances.

Keywords—Quantum Key Distribution Network, QKD link, point-to-point, secret key generation, Quantum Key Pools, key path relay, multi-commodity flow, optical switches, scheduling.

I. INTRODUCTION

In recent years, quantum computing has posed a security threat as new algorithms can exploit its power to break traditional network security practices relying on public key cryptography, such as the distribution of symmetric keys [1]. In response, research has focused on Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). We focus here on QKD which leverages quantum principles to securely distribute keys between two endpoints [2]. To enable network wide key distribution, two key QKD architectures have emerged: Relayed QKD, where intermediate nodes act as trusted relays, and Switched QKD, which uses optical switches to dynamically configure end-to-end QKD links.

In Relayed QKD (Fig. 1a), nodes in a mesh quantum fiber network establish direct QKD links with adjacent neighbors using dedicated Alice-Bob quantum device pairs. Communication between non-adjacent nodes is achieved by relaying keys through intermediate nodes, which must be trusted. Each node hosts a Key Management System (KMS) server. The KMS buffers keys generated by the node's QKD links in Quantum Key Pools (QKPs) and also manages the relays. For a key relay, keys are consumed from the QKPs using one-time-pad (OTP) encryption along the path and are stored in Virtual Quantum Key Pools (VQKPs) at the path's source and destination endnodes. This architecture requires one QKD device pair per link, so for L links, L device pairs are needed. In most networks, $L = O(N)$, where N is the number of nodes—thus Relayed requires significantly fewer devices

compared to a point-to-point quantum network. However, this design consumes more key material, as in a typical network with $O(N)$ links, a node participates on average in $O(N^2)$ relay paths. Therefore, efficient path and key flow allocation require optimized multi-commodity flow algorithms.

In Switched QKD (Fig. 1b), each node is equipped with one Alice and one Bob device, connected to an optical switch that, in turn, connects to all other nodes via the quantum network. Quantum communication between nodes can be achieved using either: (i) shared fibers, with (i.a) different wavelengths for simultaneous quantum key generation sessions, or (i.b) the same wavelength while avoiding simultaneous key sessions on fiber paths; or (ii) dedicated fibers between nodes requiring secure communication. In this paper, we consider option (ii), since fibers are typically abundant. The switches allow on-demand connection of Alice-Bob pairs across the network. Switched QKD avoids the need for trusted nodes. However, it requires arbitrary QKD device pairing, which can reduce the generated secret key rate (SKR). In experiments with commercial QKD devices, we observed significant SKR degradation when pairing non-optimized devices [3]. While only N QKD device pairs are required for N nodes, the devices are shared over time and cannot serve all pairs concurrently. Keys are generated in time-limited sessions and stored in each node's KMS server QKP for later use. Scheduling algorithms are essential to determine which QKD links to activate and for how long—especially since link distance affects the key generation rates (SKR).

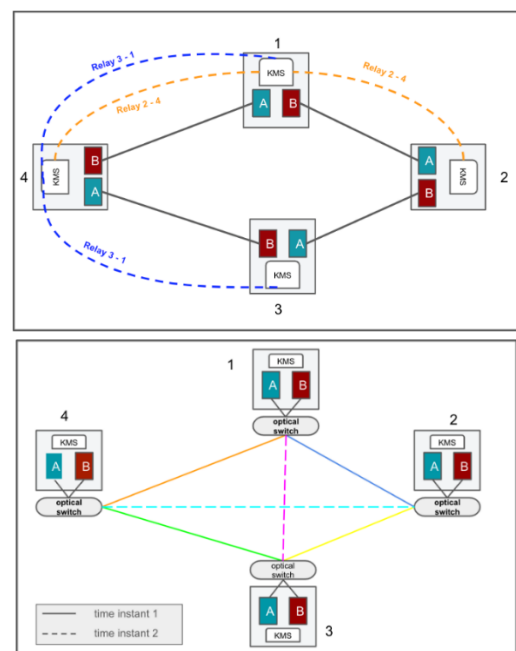


Figure: 1 Example of: a) Relayed and b) Switched QKD networks.

Relayed QKD is considered mature. Studies like [4][5] and [5] use integer linear programming (ILP) formulations for key relay optimization, showing superior performance despite high computation time as opposed to heuristics. Relayed QKD is also implemented in commercial products (e.g., IDQ Clarion [6], evolutionQ [7]). Switched QKD, though still experimental, has shown promise in trusted-node-free networks. It involves dynamic session scheduling and reconfiguring QKD links. Studies [8]–[11] propose heuristic and ILP algorithms, while some limited support has been adopted in products, e.g. in ThinkQuantum KMS [12].

To compare the Relayed and Switched QKD architectures, we derived for uniform ring networks optimal configurations and analytical formulas [3]. Our results showed that Switched QKD performs better in uniform rings with short distances and many nodes, while Relayed QKD outperforms in the long distances. We also proposed algorithms for arbitrary topologies [13] and used them to compare these architectures in more realistic non-uniform rings [14]. We reached similar conclusions for non-uniform rings. In these paper we summarize the algorithms and findings of [3][13] and [14].

II. NETWORK MODELING

In this section we discuss the Switched and Relayed QKD network architectures and the associated optimization problems. For Switched QKD, we present a generic ILP model for arbitrary topologies, which is refined with constraints to improve efficiency in ring networks. We also construct an optimal schedule for uniform rings. For Relayed QKD, we propose an LP model, based on [4], which handles both generic and ring topologies, and we also construct an optimal key relay configuration for uniform rings.

The QKD network is structured into three layers: 1) Quantum Layer – connects quantum devices (Alices/Bobs) via dedicated fibers, 2) Key Management System (KMS) – each node hosts a KMS server that buffers keys, and in Relayed QKD it forwards/relays keys, and 3) Secured Application Entities (SAEs) – use symmetric keys from KMSs to encrypt their communication. We assumed an all-to-all consumption profile, where each node has one SAE that communicates with a SAE in every other node, and the goal is to maximize the minimum key consumption rate for fairness. However, our solutions can be easily extended for arbitrary SAE demands. The KMS manages key flows and maintains separate buffers at its output per SAE pair. Key generation and SKR refers to the output from QKD devices to KMS, while consumption refers to the output of KMS and use of keys by SAEs.

A. Relayed QKD Network

In the Relayed QKD architecture, a mesh quantum network enables symmetric key generation between adjacent nodes via direct QKD links, each realized by an Alice-Bob pair. Keys from QKD link (n_i, n_j) are generated at a known SKR G_{ij} . We assume this value is available—based on historical data, modeling, or prediction—and it reflects device-specific performance and link attenuation. Generated keys are buffered into local Quantum Key Pools QKP_{ij} . For quantum-safe communication between non-adjacent nodes (n_s, n_d) , a path p_{sd} of trusted intermediate nodes is selected (the definitions can be extended to multiple paths). Each intermediate node $n_i \in p_{sd}$ operates at the KMS server, using One-Time-Pad (OTP) encryption to relay a key from n_s to n_d , using one key from the QKP of the previous link and one from

the QKP of the next links along the path. The resulting end-to-end keys are stored in Virtual Quantum Key Pools $VQKP_{sd}$ at the endpoints, from which they are consumed by the respective SAEs at a rate c_{sd} . Thus, to provision $VQKP_{sd}$, key flow rates f_{ij}^{sd} must be identified—quantifying how much key material is drawn from each QKP_{ij} to support secure communication for each demanding (s, d) SAE pair. The effective end-to-end key consumption rate c_{sd} is limited by the bottleneck link along the selected path: $c_{sd} = \min_{i,j \in p_{sd}} f_{ij}^{sd}$. This

formulation can be extended to support multiple paths for redundancy or load balancing. Thus, the KMS orchestrator determines the paths and allocates per-link key flow rates f_{ij}^{sd} subject to generation rates G_{ij} , which are keys temporary stored in QKP_{ij} . Considering rates this is formally expressed by: $G_{ij} \leq \sum_{sd} f_{ij}^{sd}$. The overall objective is to maximize the minimum achievable consumption rate across all active communication pairs: $\max c_R$ such that $c_R \leq c_{sd}, \forall (s, d)$. This is a variation of the multi-commodity flow optimization problem, common in graphs and networks.

1) LP formulation for key flow optimization in Relayed QKD over arbitrary network topologies

An ILP model was introduced in [4] to find an optimal integer flow, maximizing a weighted combination of average and minimum key generation for arbitrary topologies. We adapted that model by: (i) incorporating bidirectional traffic demands, (ii) modifying the objective to directly maximize the minimum c_R , and (iii) relaxing integer constraints to allow floating-point consumption rates, enabling a Linear Program (LP) formulation that is solved optimally in polynomial time.

1) Optimal key flow allocation for uniform rings

In a ring topology with uniform QKD link generation rates, key flow computations are simplified due to symmetry. Each node n_i communicates with remote nodes n_{i+k} via paths of exactly k hops. To maximize the minimum end-to-end key consumption rate across all source–destination (SAE) pairs, we equalize the consumption contributions f_{ij}^{sd} of each QKD link across all paths that use it. Specifically, each QKD link (n_i, n_{i+1}) supports communication for a total of $N^2 - 1/8$ distinct SAE pairs. Therefore, its generation rate $G(A^e)$, with $A^e = a_e \cdot L^e$ being the attenuation for uniform links of length L^e and a_e the attenuation coefficient, is divided equally among those pairs. The resulting uniform end-to-end key consumption rate is:

$$c_R = 8 \cdot G(A^e) / (N^2 - 1).$$

B. Switched QKD Network

We model the Switched QKD architecture assuming that each node is equipped with one Alice and one Bob device, connected to an optical switch, but we can generalize to nodes with multiple devices. Each node's optical switch is connected via dedicated fibers to every other node at the quantum communication layer (Layer 1), enabling dynamic establishment of QKD links (or key sessions) between any pair of nodes. During an active QKD link between nodes (n_i, n_j) , keys are generated at an SKR G_{ij} . We divide time into periods of fixed length T . At the beginning of each period, we assume G_{ij} is known, e.g. measured and averaged over previous periods or predicted. We schedule each QKD link (n_i, n_j) to be active once and for a duration d_{ij} within T . During this time, keys are generated and stored in end-point KMS servers' quantum key pools (QKPs).

Meanwhile, SAE pairs consume keys continuously at rate c_{ij} , even when the QKD link is deactivated. To guarantee key availability, we ensure that the generated keys meet or exceed the total consumption during T : $d_{ij}G_{ij} \geq Tc_{ij}$. Since longer links have lower key generation rates, they need to remain active longer to adequately refill the key buffers. KMS buffers have a limited capacity M (assumed uniform for simplicity), and thus: $c_{ij}(T - d_{ij}) \leq M$. Each QKD device can participate in only one active link at a time, and switching links requires a reconfiguration time R . We also include an attenuation penalty P to account for switch-related losses and QKD device mismatches. Clearly to solve this optimization a sophisticated scheduling algorithm is needed.

Fig. 2 illustrates a sample schedule and QKP buffer levels for the network in Fig. 1b. Since SKR generation varies over time, the actual key generation may differ from the input estimate, leading to discrepancies in buffer levels at the end of a period. To address this, we propose re-running the scheduling algorithm with updated SKR values before each new period. Additionally, we can define a key margin to accommodate SKR fluctuations and prevent key depletion.

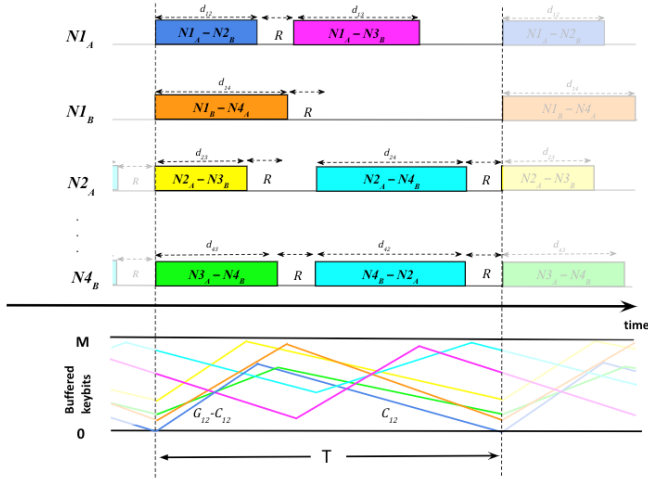


Figure 2: Schedule sample of QKD links (key generation sessions) and corresponding level of key buffers for the network of 4 nodes shown in Fig. 1.b (colors code the QKD links) for a period T .

2) ILP formulation for switched QKD over arbitrary topology and extensions for (non-uniform) rings

We developed in [13] and [14] an Integer Linear Programming (ILP) model that, given the average SKR between node pairs in a Switched QKD network, determines the start time and duration of each QKD link (key generation session) to maximize the minimum key consumption rate across all pairs. The model accounts for hardware constraints (e.g., number of Alice/Bob devices), buffer capacities, and QKD link collisions. For (non-uniform) ring networks we also introduced in [14] symmetry-breaking constraints that reduce the solution space without sacrificing solution quality.

3) Optimal scheduling for uniform rings

For uniform ring topologies, we constructed in [3] an optimal schedule that achieves fairness and efficiency in key distribution. We group all QKD links connecting k -hop distant node pairs and schedule/configure them in distinct time phases. This leverages the inherent symmetry of uniform rings: all k -hop links experience the same attenuation A^k (e.g., computed as $A^k = a_c \cdot \text{chord}(k, L^e)$, where L^e is the adjacent nodes link length and a_c the attenuation coefficient), and thus all k -

hop links have identical SKR $G(A^k)$. In each phase, the Alice at node n_i communicates with the Bob at node n_{i+k} , and the Bob at the same node n_i with the Alice at node n_{i-k} , simultaneously. Thus, to serve all-to-all pairs, we range k from 1 up to $(N-1)/2$. By allocating time to each k -hop group inversely proportional to its SKR, so $1/G(A^k)$, we ensure that all source-destination pairs achieve the same key consumption rates. The result is a periodic schedule that maximizes the minimum key rate c_s across all pairs given by:

$$c_s = \frac{1}{(R(N-1)/2) + \sum_{k=1}^{(N-1)/2} \frac{1}{G(A^k)}}$$

III. NUMERICAL RESULTS

We performed a comparison of the Relayed and Switched QKD network architectures in uniform and non-uniform rings. We assumed one Alice and one Bob device at each node. For uniform rings we used the analytical formulas outlined in Sections II.A.2 and II.B.2, while for non-uniform rings the LP and ILP formulations outlined in Sections II.A.1 and II.B.1.

We assumed ring topologies for the quantum layer, with fiber links between neighboring nodes and additional chord fiber links in the Switched architecture. The secret key generation rate (SKR) function $G()$ was modeled based on Toshiba's 4.2-MB Quantum Devices [15]. The Toshiba devices are designed to operate within a receiver dynamic range of -5 dBm to -22 dBm, requiring additional attenuators when the received power is higher than -5 dBm. Due to this, the generation function has a flat distance of 20 km, below which the SKR is flat. For QKD link (n_i, n_j) the SKR was defined in terms of the attenuation, as $G_{ij} = G(A_{ij})$, where the link attenuation $A_{ij} = a_c L_{ij}$ was proportional to the distance L_{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 L_{ij} was defined only for adjacent nodes and was equal to their distance, i.e. $L_{ij} = L^e$ for all i and j . In the Switched architecture, we assumed chord fiber links, so assuming that (n_i, n_j) are k -hops apart, $L_{ij} = L^k = \text{chord}(k, L^e)$. For Switched, we also assumed a scheduling period, $T = 180$ min, a reconfiguration time to switch between key-generation sessions (release and create a new QKD link), $R = 5$ min, and additional losses caused by the optical switches, $P = 2$ dB.

We simulated uniform rings with different numbers of nodes N ($=5, 7, 9, 13, 17, 21$), different adjacent node distances L^e ($=2.5, 5, 7.5, 10, 15, 20, 25$ km). To simulate non-uniform rings we considered L^e to be the average adjacent node distance and a distance deviation factor f , and drew the distance of each link from a uniform distribution with a range of $(L^e - L^e f, L^e + L^e f)$. We conducted simulations with different distance deviation factors f , and we present results here for $f = 0.5$. For the Switched QKD and computationally complex scenarios with $N = 17$ nodes or more, we stopped the simulation after 2 hours. To compare the optimal consumption rate of Switched QKD (c_s) with that of Relayed QKD (c_r), we introduce a relative consumption performance metric ρ , defined as:

$$\rho = 100 \cdot (c_s - c_r) / \max(c_s - c_r).$$

The metric ρ ranges from -100 (Relayed outperforms) to +100 (Switched outperforms). For non-uniform rings, and for each specific combination of (N, L^e, f) , we computed the consumption rates, calculated ρ , and averaged it over 10 random scenarios (adjacent node distances drawn with

uniform distribution) per parameter set. For uniform rings, a single instance exists and was evaluated for each (N, L^e) .

A. Comparison in Uniform Rings

Fig. 3 shows the relative performance of the Switched and Relayed QKD architectures for indicative ring scenarios ($N=5$ to 21 nodes, and $L^e = 2.5$ to 25 km distance). Switched consistently outperforms Relayed in rings with short distances between nodes. In general, at short distances, the flat key generation distance (constant SKR below 20 km) limits Relayed's performance. For $N=5$ nodes and all distances the improvement remains stable due to the flat generation function distance. The Switched architecture performs relatively better ($f > 25$), for ($L^e \leq 7.5$ km and $N \leq 13$), and for ($L^e \leq 5$ km and all examined N). The improvement becomes significant ($f > 50$), in large networks with short distances ($N \geq 17$ and $L^e < 5$). On the other hand, Relayed outperforms ($f < -50$) Switched in scenarios of small networks ($N=9$ and $L^e > 20$ km), medium sized networks ($N=13, 17$ and $L^e > 15$ km), and large networks ($N=21$ and $L^e > 10$ km). Moreover, Relayed is relatively better ($f < -25$) for ($N=5$ and $L^e=25$ km), ($N=17$ and $L^e=10$ km), and ($N=21$ and $L^e=7.5$ km). The in-between scenarios fall in a gray zone where neither Switched nor Relayed QKD is notably better.

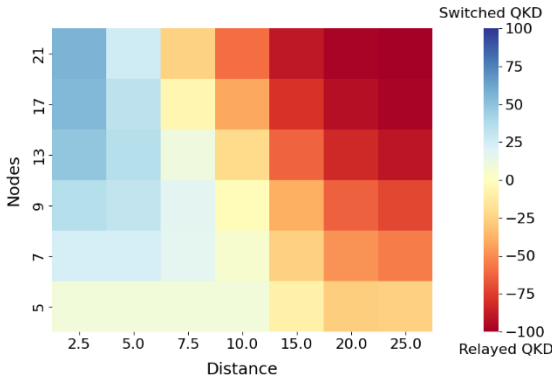


Figure 3: Relative consumption performance of Switched and Relayed architecture in uniform rings with varying nodes count (N) and adjacent nodes distance (L^e).

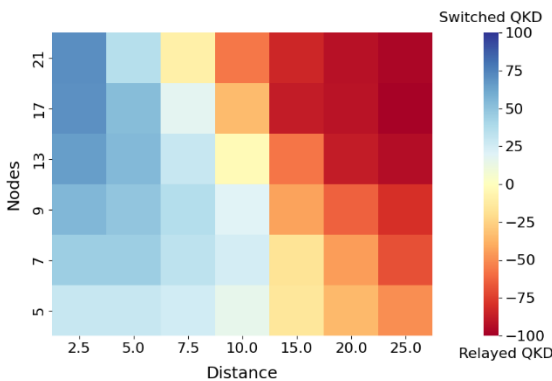


Figure 4: Average relative consumption performance rate of Switched and Relayed architecture in non-uniform rings for various length distances L , number of nodes N and a distance deviation factor $f=0.5$.

B. Comparison for Non-Uniform Rings

Fig. 4 shows the average relative consumption performance for non-uniform rings and a deviation factor of $f=0.5$. The results are aligned with those in uniform rings. Switched QKD shows superior performance in scenarios with short distances and a large number of nodes. This advantage arises because

Switched scales better with the number of nodes (N), and especially at short distances where the SKR is constant below 20 km, limiting Relayed's performance. For longer distances, ($L \geq 20$ km and $N \geq 7$ nodes), ($L \geq 15$ km and $N \geq 9$), and ($L \geq 10$ km and $N \geq 17$), the Relay QKD architecture outperforms Switched. In intermediate scenarios, both algorithms must be run for a specific ring to identify the better option.

IV. CONCLUSIONS

To support scalable quantum key distribution, two architectures are commonly considered: Relayed QKD, which relays keys over multi-hop trusted-node paths, and Switched QKD, which uses optical switches to dynamically pair QKD modules, enabling direct end-to-end key distribution. We proposed algorithms to manage the keys in Relayed and Switched QKD for arbitrary topologies that cover also non-uniform rings, but also optimal configurations for uniform rings. We then compared these architectures in uniform and non-uniform rings. Our results show that Switched QKD outperforms in short-distance, large-node-count networks, while Relayed QKD is more effective in long-distance, large-node-count networks. A hybrid approach could combine the advantages of both architectures—maximizing security, performance, and flexibility.

ACKNOWLEDGMENT

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.

REFERENCES

- [1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", Annual Symposium on Foundations of Computer Science, 1994.
- [2] Chip Elliott, "Building the quantum network", New J. Phys, 2002.
- [3] N. Makris et. al., "Relayed-QKD and switched-QKD networks performance comparison considering physical layer QKD limitations", OFC, 2024.
- [4] C. Lee et. al., "Key-count differential-based proactive key relay algorithm for scalable quantum-secured networking", Journal of Optical Communications and Networking, vol. 15, no. 5, 2023.
- [5] T. Johann et. al., "Comparison and optimization of different routing methods for meshed QKD networks using trusted nodes", Journal of Optical Communications and Networking, vol. 16, no. 3, 2024.
- [6] www.idquantique.com/quantum-safe-security/products/clarion-kx-platform/
- [7] www.evolutionq.com/products/basejumpqdn
- [8] Y. Cao, et. al., "Time-Scheduled Quantum Key Distribution (QKD) Over WDM Networks", Journal of Lightwave Technology, 2018.
- [9] O. Alia et. al., "Dynamic DV-QKD Networking in Trusted-Node-Free Software-Defined Optical Networks", Journal of Lightwave Technology, vol. 40, no. 17, 2022.
- [10] 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.
- [11] 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.
- [12] www.thinkquantum.com/wp-content/uploads/files/Brochure_QUKY.pdf
- [13] K. Christodoulou, et. al., "Optimizing Key Consumption in Switched QKD Networks", OFC, 2024.
- [14] A. Selentis, K. Christodoulou, G. Kanellos, "Relayed vs. Switched QKD: A Comparison in Non-uniform Ring Networks", ONDM 2025.
- [15] www.global.toshiba/ww/products-solutions/security-ict/qkd/products.html