OPEN ACCESS

Topological optimization of quantum key distribution networks

New Journal of Physics
The open-access journal for physics

Topological optimization of quantum key distribution networks

R Alléaume[1,4], F Roueff[1], E Diamanti[1] and N Lütkenhaus[2,3]

[1] Telecom ParisTech and LTCI—CNRS, Paris, France
[2] University of Erlangen, Germany
[3] Institute for Quantum Computing, Waterloo, Canada
E-mail: romain.alleaume@telecom-paristech.fr

New Journal of Physics **11** (2009) 075002 (24pp)
Received 3 March 2009
Published 2 July 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/7/075002

Abstract. A quantum key distribution (QKD) network is an infrastructure that allows the realization of the key distribution cryptographic primitive over long distances and at high rates with information-theoretic security. In this work, we consider QKD networks based on trusted repeaters from a topology viewpoint, and present a set of analytical models that can be used to optimize the spatial distribution of QKD devices and nodes in specific network configurations in order to guarantee a certain level of service to network users, at a minimum cost. We give details on new methods and original results regarding such cost minimization arguments applied to QKD networks. These results are likely to become of high importance when the deployment of QKD networks will be addressed by future quantum telecommunication operators. They will therefore have a strong impact on the design and requirements of the next generation of QKD devices.

[4] Author to whom any correspondence should be addressed.

Contents

1. Introduction

Quantum key distribution (QKD) is a technology that uses the properties of quantum mechanics to realize an important cryptographic primitive: key distribution[5]. Unlike the techniques used in traditional 'classical' cryptography, for which the security relies on the conjectured computational hardness of certain mathematical problems, QKD security can be formally proven. Secret keys established via QKD are information-theoretically secure, which implies that any adversary trying to eavesdrop cannot obtain any information on the transmitted keys at any point in the future, even if she possesses extremely large computational resources.

The communication channels needed to perform QKD consist of an optical channel, on which well-controlled quantum states of light are exchanged, and a classical channel that is used for signaling during the quantum exchanges and for the classical post-processing phase, namely key reconciliation. Their combination forms a communication link, over which QKD allows two distant users to exchange a specific type of data, in particular secret keys. In this sense, QKD is by nature a telecommunication technology, and so *QKD links* can be combined with appropriately designed nodes to form *QKD networks*.

The performance of QKD links has rapidly improved in the last years. Starting from pioneering experiments in the 1990s [1], important steps have been taken to bring QKD from the laboratory to the open field. Thanks to the continuous efforts invested in developing better QKD protocols and hardware, in parallel to the advancement of security proofs (see [2]–[4] for reviews), the performance that can now be achieved, in terms of attainable communication distance, secret key generation rate and reliability, positions

[5] More accurately, the primitive is that of secret key agreement using a public quantum channel and a public authenticated classical channel.

QKD as the first quantum information processing technology reaching a level of maturity sufficient to target deployment over real-world networks. Indeed, off-the-shelf QKD systems are now commercially available [5], and the first QKD networks have recently been implemented [6]–[8].

Up till now, research in QKD has focused on building and optimizing individual systems to reach the longest possible distance and/or the highest possible secret bit rate, without taking into account the cost of such systems. However, as the perspective of deploying QKD networks becomes a reality, the question of optimal resource allocation, intrinsically linked to cost considerations, becomes relevant and important, as is the case for any telecommunication network infrastructure. It therefore becomes necessary to consider QKD from a cost perspective, and in particular study the potential trade-offs of cost and performance that can occur in this context.

Following the above arguments, we consider in this work the design of QKD networks from a topology viewpoint, and present techniques and analytical models that can be used to optimize the spatial distribution of QKD devices and QKD nodes within specific network architectures in order to guarantee a given level of service to the network users, at a minimum cost. We also study how cost minimization arguments influence the optimal working points of QKD links. We show in particular that, in the perspective of QKD networks, individual QKD links should be operated at an optimal working distance that can be significantly shorter than their maximum attainable distance.

This paper is structured as follows. In section 2, we define a QKD network and discuss the topology and characteristics of the network architecture that we consider in this work. We also introduce the concept of a backbone network structure. In section 3, we present our calculations and results on network topological optimization based on cost arguments. In particular, we provide a comprehensive set of modeling tools and cost function calculations in specific network configurations, and discuss the effect of our results on the design of practical QKD networks. Finally, in section 4, we discuss open questions and future perspectives for QKD networks.

2. QKD networks

2.1. Definition and types of QKD networks

Extending the range of QKD systems to very long distances, and allowing the exchange of secret keys between multiple users necessitates the development of a network infrastructure connecting multiple individual QKD links. Indeed, QKD links are inherently only adapted to point-to-point key exchange between the two endpoints of a quantum channel, while the signal-to-noise ratio decrease occurring with propagation loss ultimately limits their attainable range. It is then natural to consider QKD networks as a means to overcome these limitations.

A QKD network is an infrastructure composed of QKD links, i.e. pairs of QKD devices linked by a quantum and a classical communication channel connecting two separate locations, or nodes. These links are then used to connect multiple distant nodes. Based on these resources and using appropriate protocols, this infrastructure can enable the unconditionally secure distribution of symmetric secret keys between any pair of legitimate users accessing the network.

QKD networks can be categorized in two general groups [9]: networks that create an end-to-end quantum channel between the two users, and networks that require transport of the key

over many intermediate trusted nodes. In the first group, we find networks in which a classical optical function such as switching or multiplexing is applied at the node level on the quantum signals sent over the quantum channel. This approach allows multi-user QKD but cannot be used to extend the key distribution distance. Much more advanced members of this group are the quantum repeater-based QKD networks. Quantum repeaters [10] can create a perfect end-to-end quantum channel by distributing entanglement between any two network users. The implementation of quantum repeaters, however, requires complex quantum operations and quantum memories, whose realization remains an experimental challenge. The same is true for the simpler version of quantum repeaters, namely quantum relays [11], which on the one hand do not require a quantum memory but on the other cannot arbitrarily extend the QKD communication distance.

2.2. Trusted repeater QKD networks: characteristics and assumptions

In this work, we are interested in the second group of networks, which we call *trusted repeater QKD networks*. In these networks, the nodes act as trusted relays that store locally QKD-generated keys in classical memories, and then use these keys to perform long-distance key distribution between any two nodes of the network. Therefore, trusted repeater QKD networks do not require nodes equipped with quantum memories; they only require QKD devices and classical memories as well as processing units placed within secure locations, and can thus be deployed with currently available technologies. Indeed, the implementation of such networks has been the subject of several international projects [7, 8, 12, 13].

As we will see in detail in the following section, the analysis of trusted repeater QKD networks from a topology viewpoint and with the goal of achieving optimization based on cost considerations involves modeling several characteristics of such a network, namely the *user distribution*, the *node distribution*, the *call traffic* and the *traffic routing*. The user and node distributions, denoted by Π and M, respectively, will be considered as Poisson stochastic point processes, and will be thus modeled using convenient stochastic geometry tools. Modeling the traffic demand is particularly subtle because of the variation with respect to time and distance that this traffic may feature in a real network. Calculations here will neglect these variations and will be performed under the assumption of a uniform call volume between any pair of users, denoted as V.

Finally, routing in trusted repeater QKD networks is performed according to the following general principle: first, local keys are generated over QKD links and are stored in nodes that are placed on both ends of each link. Global key distribution is then performed over a QKD path, i.e. a one-dimensional (1D) chain of trusted relays connected by QKD links, establishing a connection between two end nodes. Secret keys are forwarded, in a hop-by-hop fashion, along these QKD paths. To ensure their secrecy, one-time pad encryption and information-theoretically secure authentication, both realized with a local QKD key, are performed. End-to-end information-theoretic security is thus obtained between the end nodes, provided that the intermediate nodes can be trusted.

2.3. Quantum backbone network architecture

Introducing hierarchy into network design can be an extremely convenient architectural tool because it allows us to break complex structures into smaller and more flexible ensembles.

Indeed, such hierarchical levels offer an efficient way to help solve resource allocation problems arising in networks, ranging from network routing to network deployment planning. In this work, we will associate the notion of hierarchy in QKD networks with the existence of what we will call a *quantum backbone network*.

In classical networks and especially the Internet, a backbone line is a larger transmission line that carries data gathered from smaller lines that interconnect with it. By analogy with this definition, the backbone QKD network is an infrastructure for key transport that gathers the traffic of secret key from many individual QKD links. QKD backbone links and nodes clearly appear as mutualized resources shared to provide service to many pairs of users. Keeping the fruitful analogy with classical networks, we will call *access QKD links* the point-to-point links used to connect QKD end users to their nearest QKD backbone node.

The principle of traffic routing that we described above can be conveniently transposed in the context of backbone networks. In this case, traffic from individual users is gathered locally to backbone QKD nodes. This mutualized traffic is then routed hop-by-hop over the backbone structure. Furthermore, it is important to note that the node and user point process distributions are distinct when a backbone network is considered, which might not be the case in a network without backbone.

In the following, we will derive cost functions for different QKD network configurations, under the above assumptions regarding the topology and the way traffic is routed in these networks, and as a function of the characteristics of individual QKD links. We will then use the results to discuss how QKD networks should be dimensioned, the optimal working points of QKD links, as well as the interest of adopting a hierarchical architecture, materialized by the existence of a backbone, in QKD networks.

3. Topological optimization based on cost arguments

3.1. QKD links: characterizing the rate versus distance

The main element underlying the cost optimization related to the deployment of quantum networks is the intrinsic performance of QKD links. This performance can essentially be summarized by the function $R(\ell)$, which gives the rate, in bit s^{-1}, of secret key that can be established over a QKD link of length ℓ.

Clearly, this secret key bit rate varies from system to system and comparisons between systems are thus difficult to establish. Moreover, comparisons have to be related to the security proofs for which the secret key bit rates have been derived. Security proofs are not yet fully categorized, although important steps in this direction have been taken [4].

As shown in figure 1, the typical curve describing the variation with distance of the logarithm of the mean rate of secret bit establishment $R(\ell)$ can be essentially separated into two parts:

- A **linear** part that is the region where the rate of secret key establishment varies as a given power of the propagation attenuation. Since the attenuation $\eta(\ell)$ is exponentially increasing with distance, $\log R(\ell)$ is linear in ℓ.
- An **exponential drop-off** at longer distances, where the error rate rapidly increases due to the growing contribution of detection dark counts. In this region, the decrease of the secret key rate is multiexponential with distance. The slope of the curve representing $\log R(\ell)$ is thus becoming increasingly steep until a maximum distance is reached.

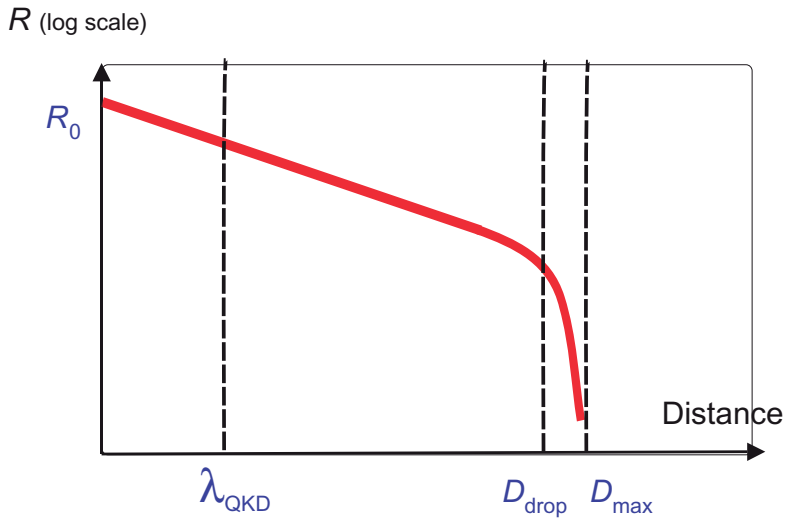

Figure 1. Typical profile of the rate versus distance curve for a single QKD link.

For completeness, it is also important to mention the possibility that, for short distances, the secret bit rate could be limited by a saturation of the detection setup. This will be the case if the repetition rate at which the quantum signals are sent in the quantum channel exceeds the bandwidth of the detector. We will, however, not investigate this possibility any further in the remaining of this work.

The behavior of the secret bit rate function $R(\ell)$ can be described using essentially three parameters, schematically shown in figure 1:

1. the secret bit rate at zero distance, R_0;
2. the scaling parameter λ_{QKD} in the linear region such that $R(\ell) = R_0\, \mathrm{e}^{-\ell/\lambda_{\mathrm{QKD}}}$; and
3. the distance at which the scaling of the rate becomes exponential, which is comparable with the maximum attainable distance, $D_{\mathrm{drop}} \sim D_{\mathrm{max}}$.

R_0 is determined by the maximum clock rate of the QKD system. In QKD relying on photon-counting detection setups, R_0 is limited by the performance of the detectors, and is usually in the Mbit s^{-1} range. Clearly, the solutions allowing to improve the performance of the detectors have a direct impact on R_0 [14]–[17]. For QKD systems relying on continuous variables [18], based on homodyne detection performed with fast photodiodes, the experimental bound on R_0 can be significantly higher, potentially in the Gbit s^{-1} range. The computational complexity of the reconciliation, however, currently limits R_0 in the Mbit s^{-1} range in the practical demonstrations performed so far [19].

The scaling parameter λ_{QKD} is essentially determined by the attenuation $\eta(\ell)$ over a quantum channel of length ℓ, and by a coefficient r that is mainly related to the security proof that can be applied to the experimental system. In the case of a typical network based on optical fibers, the attenuation $\eta(\ell)$ can be parameterized by an attenuation coefficient α (in dB km^{-1}) as $\eta(\ell) = 10^{-\alpha\ell/10}$ (for scaling of the attenuation in free space, see [4]). In the linear part of the curve shown in figure 1, the rate $R(\ell)$ varies as a given power r of the attenuation, $R(\ell) = R_0\, \eta(\ell)^r$. We can thus define the scaling parameter as $\lambda_{\mathrm{QKD}} = 10/(\alpha\, r \log(10))$.

For QKD performed at telecom wavelengths, with protocols optimized for long distance operation, we can take $\alpha = 0.22\,\mathrm{dB\,km^{-1}}$ and $r = 1$, which leads us to $\lambda_{\mathrm{QKD}} = 19.7\,\mathrm{km}$, as the typical scaling distance for such QKD systems. This parameter is important since, as we shall see in the following, the optimal working distance of QKD links will essentially scale as λ_{QKD}.

Finally, the existence of a rapid drop-off of the secret key rate at distances around D_{drop} arises when the probability to detect some signal sent in the quantum channel, p_{s}, becomes comparable with the probability to detect a dark count per detection time slot, p_{d}. This occurs around the distance D_{drop}, for which we have $p_{\mathrm{s}} \simeq \exp(-D_{\mathrm{drop}}/\lambda_{\mathrm{QKD}})\eta_{\mathrm{d}}$, where η_{d} represents the detector efficiency. We thus find $D_{\mathrm{drop}} \simeq \lambda_{\mathrm{QKD}} \log(\eta_{\mathrm{d}}/p_{\mathrm{d}})$. In practice, when working with InGaAs single-photon avalanche photodiodes (SPADs) operating at 1550 nm, the ratio $\eta_{\mathrm{d}}/p_{\mathrm{d}}$ is optimized by varying the different external parameters of the detector such as the temperature, gate voltage or time slot duration. The best published performances for InGaAs SPADs [20, 21] report values of the dark counts $p_{\mathrm{d}} \simeq 10^{-7} - 10^{-6}$ for a detection efficiency η_{d} around 10%, which leads to $D_{\mathrm{drop}} \sim D_{\mathrm{max}} \sim 100$–$120\,\mathrm{km}$ for QKD systems employing such detectors. For a similar detection efficiency, the best available superconducting single-photon detectors (SSPDs) present dark counts $p_{\mathrm{d}} \simeq 10^{-8} - 10^{-6}$ [22], leading to a maximum distance that can reach 140 km.

3.2. Toy model for QKD network cost derivation: a linear chain between two users

3.2.1. The linear chain as a simple asymptotic model of a quantum backbone network. As a first example of QKD network cost derivation and optimization, we will consider what we will call the linear chain scenario. In particular, we consider two users, A and B, that want to rely on QKD to exchange secret keys in a scenario that imposes the use of several QKD links:

- The two QKD users are *very far away*: their distance is $L = \| AB \|$ with $L \gg D_{\mathrm{max}}$.
- The two QKD users are exchanging secret bits at a *very high rate*. We will call V the volume of calls between the two users A and B (units of V: bits of secret key), and will assume $V \gg R_0$.

Because of the first condition, many intermediate nodes have to be used as trusted key relays to ensure key transport over QKD links from A to B. Because of the second condition, many QKD links have to be deployed in parallel to reach a secret key distribution rate capacity at least equal to the traffic volume.

The linear chain QKD network scenario is in a sense the simplest situation in which an infrastructure such as a quantum backbone network, described in section 2, is required. It therefore provides an interesting toy model for cost optimization and topological considerations.

3.2.2. Cost model: assumptions and definitions. The generic purpose of cost optimization is to ensure a given objective in terms of service, at the minimum cost. In the case of the linear chain scenario, this objective is to be able to offer a secret bit rate of V bit $\mathrm{s^{-1}}$ between two users A and B separated by a distance L, while minimizing the cost of the network infrastructure to be deployed.

In this and all subsequent models, we will consider as the total cost $\mathcal{C}$ of a QKD network, the cost of the equipment to be deployed to build the network. This can be seen as a simplifying assumption, since it is common, in network planning, to differentiate between capital and

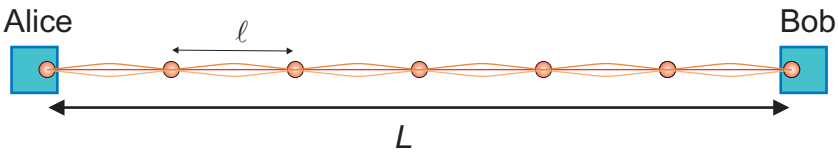

Figure 2. The 1D QKD chain linking two QKD users, Alice and Bob, over a distance L. Since L is considered much longer than the maximum span of a QKD link, $D_{\max}$, intermediate QKD nodes are needed to serve as trusted relays.

operating expenditures. We have chosen here to restrict our models to capital expenditures of QKD networks and will consider that their cost is arising from two sources:

- The cost of QKD link equipment to be deployed. We will denote as C_{QKD} the unit cost per QKD link. C_{QKD} essentially corresponds to the cost of a pair of QKD devices. Note that here we implicitly assume that the deployment of optical fibers is *for free*, or more precisely that it is done independently and prior to the deployment of a QKD network.
- The cost of node equipment, which we denote as C_{node}. C_{node} typically corresponds to the hardware cost (for example, some specific kind of routers need to be deployed inside QKD nodes), as well as the cost of the security infrastructure that is needed to make a QKD node a trusted and secure location.

As explained before and shown in figure 2, a linear chain QKD network is composed of a 1D chain where adjacent QKD nodes are connected by QKD chain segments, each segment being potentially composed of multiple QKD links to ensure that a capacity equal to the traffic volume is reached.

3.2.3. Total cost of the linear chain QKD network. For convexity reasons, discussed in more detail at the end of this section, the topology ensuring the minimum cost will correspond to place QKD nodes at regular intervals between A and B. We denote by ℓ the distance between two intermediate nodes, which then corresponds to the distance over which QKD links are operated within the linear chain QKD network. As we shall see, the question of cost minimization will reduce to finding the optimum value of QKD link operational distance, ℓ^{opt}, for the linear chain QKD network.

There are clearly two antagonistic effects in the dependence of the total cost of the considered network on ℓ:

- On the one hand, if QKD links are operated over long distances, their secret bit capacity $R(\ell)$ decreases. This will impose the deployment of more QKD links in parallel, on each chain segment linking two adjacent QKD nodes, and thus tends to increase the total cost.
- On the other hand, it is clear that increasing the operating distance ℓ allows us to decrease the required number of intermediate trusted relay nodes, which leads to a decreased cost.

The optimum operating distance ℓ^{opt} corresponds to the value of ℓ that minimizes the total cost function $\mathcal{C}$:

$$\mathcal{C} = C_{\mathrm{QKD}} \frac{L}{\ell} \frac{V}{R(\ell)} + C_{\mathrm{node}} \frac{L}{\ell}. \tag{1}$$

It is important to note that, in the above equation, we have made the assumption that we can neglect the effects of discretization. This means that the length of the chain, L, can be considered much longer than the length of individual QKD links, ℓ, and that the traffic volume V can be considered as a continuous quantity, neglecting the discrete jumps associated with variations in the number of calls.

3.2.4. Cost minimization and optimum working distance of QKD links. In the asymptotic limit of very high traffic volume V, the cost of nodes can be neglected in comparison with the cost of QKD devices. The expression of the total cost in equation (1) then reduces to the first term, and we have the following interesting properties:

- The total cost is directly proportional to the product of the traffic volume V and the total distance L.
- Optimizing the total cost $\mathcal{C}$ is equivalent to minimizing $C(\ell)/\ell$ where $C(\ell) = C_{\mathrm{QKD}}/R(\ell)$ is the per-bit cost of one unit of secret key rate.

Furthermore, assuming that QKD links are operated in the linear part of their characteristic (see figure 1), we can write $C(\ell) = \frac{C_{\mathrm{QKD}}}{R_0} \mathrm{e}^{\ell/\lambda_{\mathrm{QKD}}}$. Then, the value of ℓ^{opt} that minimizes the quantity $C(\ell)/\ell$ can be explicitly derived as

$$\ell^{\mathrm{opt}} = \lambda_{\mathrm{QKD}}, \tag{2}$$

where λ_{QKD} was defined in section 3.1 as the natural scaling parameter of the function $R(\ell)$.

In the general case, the second term of the cost function in equation (1), corresponding to the cost of nodes, cannot be neglected. This second term does not depend on the volume of traffic V, and is always decreasing with ℓ. As a consequence, the optimum operating distance that minimizes $\mathcal{C}$ will always be greater than λ_{QKD}, the value minimizing the first term in equation (1).

Under the assumption that the optimum distance will remain in the linear part of the function $\log R(\ell)$, we can derive the following implicit relation for ℓ^{opt}:

$$\ell^{\mathrm{opt}} = \lambda_{\mathrm{QKD}} \left(1 + \frac{C_{\mathrm{node}}}{C_{\mathrm{QKD}}} \frac{R_0}{V} \mathrm{e}^{-\ell^{\mathrm{opt}}/\lambda_{\mathrm{QKD}}}\right). \tag{3}$$

The above equation allows for a quantitative discussion of the 'weight' of the nodes in the behavior of the cost function. Indeed, we can see that the influence of the node cost is potentially important and can lead to an optimum working distance that can be significantly greater than λ_{QKD} when $\frac{C_{\mathrm{node}}}{C_{\mathrm{QKD}}} \frac{R_0}{V} \gg 1$.

3.2.5. Existence of an optimum working distance and convexity of $C(\ell)$. In most of the explicit derivations performed in this work, we assume a purely linear dependency of $\log R(\ell)$ on ℓ. This assumption is convenient but remains an approximation since it does not take into account the drop-off of $R(\ell)$ occurring around D_{drop}.

It is, however, possible to demonstrate the existence of an optimum working distance for QKD links in a more general case, by solely relying on the assumption that the function $R(\ell)$ is log-concave, i.e. that $\log R(\ell)$ is concave. The log-concavity of $R(\ell)$ can be checked on a simple model inspired by the secret key rate formula for the BB84 QKD protocol with perfect single photons [4]. In particular, in this case we have $R(p) = 1 - 2\,h(p)$, where $h(p)$ is the entropy

associated with a quantum bit error rate p, and assume that the dependence of the error rate p on the distance is of the form $p = a + b/\eta(\ell) = a + b^{\ell/\lambda_{\mathrm{QKD}}}$, where a and b are parameters linked to the detection system. In this setup, it is straightforward to verify numerically that $\log R(\ell)$ is concave for all reasonable values of a and b.

Since $C(\ell)$, the per-unit cost of secret bit rate on a QKD link, is proportional to $1/R(\ell)$, the log-concavity of $R(\ell)$ implies the log-convexity of $C(\ell)$, which itself implies the convexity of $C(\ell)$. Finally, we can write the total cost of the linear chain QKD network as the sum of the cost of each chain segment and the cost of the node equipment, namely

$$\mathcal{C}(\ell_0, \ldots, \ell_n) = V \sum_{i=0}^{n} C(\ell_i) + n\, C_{\mathrm{node}}.$$

In the above equation, ℓ_0 denotes the distance between A and the first node, $\ell_k, k = 1, \ldots, n-1$, the distance between the kth node and the $k+1$th node, and ℓ_n the distance between the last node and B. For a convex function C, the minimization of $\sum_{i=0}^{n} C(\ell_i)$ under the constraint $\sum_{i=0}^{n} \ell_i = L$, where L is the distance between A and B, is obtained with $\ell_i = L/(n+1)$ for all i. Once we set $\ell_i = L/(n+1)$, the cost expression in the above equation only depends on n, or equivalently on $\ell = L/(n+1)$. For large L, we can disregard the fact that ℓ is an integer divider of L and approximate $(n+1)/n$ by 1, which then leads to equation (1).

3.3. Cost of QKD networks: toward more general models

The linear chain toy model developed in section 3.2 provides an interesting intuition into the behavior of the cost function. The most important result is that, in the limit of large traffic rates and/or low cost of QKD nodes, the QKD network cost optimization reduces to the minimization of $C(\ell)/\ell \sim 1/(R(\ell)\ell)$. This leads to the existence of an optimum working distance, ℓ^{opt}, at which QKD links need to be operated in order to minimize the global cost of the network deployment.

The linear chain QKD network model is, however, too restrictive in many aspects: it is 1D and limited to the description of a network providing service to two users. We will now consider more general models, which allow us to study the more realistic case of QKD networks spanning a 2D area, and providing service to a large number of users.

3.3.1. Modeling network spatial processes with stochastic geometry. Stochastic geometry is a very useful mathematical tool for modeling telecommunication networks. It has the advantage of being able to describe the essential spatial characteristics of a network using a small number of parameters [23]. It thus allows us to study some general characteristics of a given network, like the behavior of its cost function, under a restricted set of assumptions. This approach fits well with the objectives of this work, and so we have employed stochastic tools to model a QKD backbone network.

As we shall see, instead of calculating the cost of a QKD network for fixed topologies and traffic usage, we will try to understand the general behavior of the cost function by calculating the *average* cost function, where the average will be taken over some probability distributions of spatial processes modeling QKD users and QKD node locations.

The collection of spatial locations of the QKD nodes over the plane will be represented by a spatial point process $M = \{X_i\}$. Then, as illustrated in figure 3, we define a corresponding

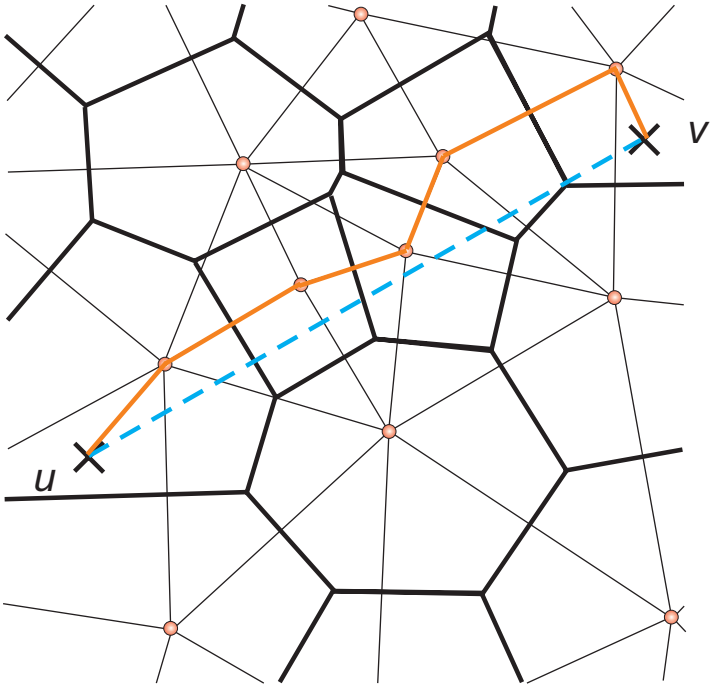

Figure 3. Thick black lines: Voronoï partition associated to a given distribution of nodes. Thin black lines: the Delaunay graph, connecting the center of neighboring Voronoï cells. In the backbone QKD network model, backbone QKD links will indeed correspond to the Delaunay graph, while backbone nodes correspond to the nucleus of the Voronoï cells. We have also represented in the same figure a typical end-to-end path, between two QKD users u and v, under the Markov-path routing policy (see text in section 3.6.2 for details).

partition of the plane[6] as the ensemble of the convex polygons $\{D_i\}$, known as the Voronoï cells of nucleus $\{X_i\}$. Each Voronoï cell D_i is constructed by taking the intersection of the half-planes bounded by the bisectors of the segment $[X_i, X_j]$ and containing X_i. The system of all the cells creates the so-called Voronoï partition. Finally, we define the Delaunay graph as the graph, whose vertices are the $\{X_i\}$ and whose edges are formed by connecting each Voronoï cell nucleus $\{X_i\}$ with the nuclei of the adjacent Voronoï cells.

3.3.2. User distribution and traffic. In the remaining of this paper, and in contrast to the linear chain toy model developed in section 3.2, we will consider QKD networks providing secret key distribution service to a large number of users, distributed over a 2D area.

The user distribution will be modeled by a Poisson stochastic point process, $\Pi = \{U_i\}$, defined over the support D of size $L \times L$, while the average number of QKD users will be denoted by μ. The point process Π will also be assumed to have an intensity density f satisfying $\mu = \int f < \infty$, which means that for every set E the number of users within E is a Poisson random variable with mean $\int_E f$.

[6] More accurately, the geometrical object we consider here is a tesselation, the boundaries of which are neglected.

Finally, whenever this additional assumption will prove to be useful to perform the desired calculations, we will consider that the distribution of users is homogeneous over D, i.e. that the intensity function f is constant over D. We will denote this constant user density by $1/\alpha_u^2$ so that α_u corresponds to a distance (it can be shown that for large L, $\alpha_u/2$ is the average distance between the origin and the point U_i closest to the origin). We will have in this case:

$$\mu = \int f = (L/\alpha_u)^2 . \tag{4}$$

For the traffic model, we will generalize the assumption made for the linear chain QKD network model: the traffic between any pair of QKD users will be seen as an aggregate volume of calls (expressed in units of secret key exchange rate). The volume of traffic will be assumed to be the same between any pair of users, and will be denoted by V.

3.3.3. QKD networks with or without a hierarchical architecture. As was discussed in section 2, it is interesting to study to which extent deploying a structure such as a backbone, which is synonymous to the existence of hierarchy in a network, would be advantageous in the case of QKD networks. To this end, continuing to place ourselves in the perspective of cost optimization, we will derive cost functions for QKD network models with or without a quantum backbone. The obtained results will then allow us to establish comparisons and thus discuss the interest of hierarchy in quantum networks.

3.4. Cost function for a 2D network without backbone: the generalized QKD chain model

A direct way to generalize the two-user 1D chain model presented in section 3.2 is simply to assume that a chain of QKD links and intermediate nodes will be deployed between each pair of users u and v within the QKD network. Each chain will therefore be dimensioned in order to accommodate a volume V of calls. The routing of calls is trivial on such a network. The distance between the intermediate nodes on a chain will be denoted by ℓ, as in section 3.2.

Here as well, we neglect the effects of discretization, i.e. the length of the chains, $\|u - v\|$, will be considered much longer than the length of individual QKD links, ℓ, and the traffic volume V will be considered a continuous quantity. Under these assumptions, we know that the cost associated with a pair of users located respectively at positions u and v and exchanging a volume V of calls is (see equation (1))

$$\mathcal{C}^{\text{pair}}(u, v) = V\|u - v\|C(\ell)/\ell + (\|u - v\|/\ell)C_{\text{node}}. \tag{5}$$

Recall that the distribution of users is described by a Poisson point process $\Pi = \{U_i\}$. Then, we can calculate the average total cost of the QKD network, $\mathcal{C}$, by summing up the costs $\mathcal{C}^{\text{pair}}(U_k, U_l)$ associated with the QKD chains deployed between each pair of users over $k \neq l$

and then average this sum over the stochastic user point process Π:

$$\begin{aligned}\mathcal{C} &= \mathbb{E}\left[\sum_{k\neq l} \mathcal{C}^{\text{pair}}(U_k, U_l)\right] \\ &= \mathbb{E}\left[\sum_{k\neq l} V\,\|U_k - U_l\|\,C(\ell)/\ell + \|U_k - U_l\|\,C_{\text{node}}\right] \\ &= (VC(\ell)/\ell + C_{\text{node}}/\ell)\,\delta, \end{aligned} \tag{6}$$

where δ is the average sum of distances over all pairs of two different users, namely

$$\delta = \mathbb{E}\left[\sum_{k\neq l} \|U_k - U_l\|\right]. \tag{7}$$

For a homogeneous Poisson point process Π with spatial density of users α_{u}^{-2} over a square domain D of size $L \times L$, it is possible to perform the exact integral calculation of δ, yielding

$$\delta = \gamma L^5/\alpha_{\text{u}}^4 \quad \text{with} \quad \gamma = \frac{1}{3}\log(1+\sqrt{2}) + \frac{2+\sqrt{2}}{15} \simeq 0.5214. \tag{8}$$

3.5. Cost function for a 2D QKD network with backbone

The backbone architectures we will consider in this work are *topological*: for a given distribution of QKD nodes, which will be either deterministic (section 3.6.1) or stochastic (section 3.6.2), the backbone cells and backbone links will strictly coincide with the Voronoï cells and the edges of the corresponding Delaunay graph defined above, respectively.

3.5.1. Routing traffic over a QKD backbone network. The backbone hierarchical structure provides a convenient way to solve the routing problem that we have adopted in our cost calculations. For a given origin-destination pair of users (A,B) wishing to exchange a volume of calls V_{AB}, the traffic is routed in the following way:

- The traffic goes from A to its nearest QKD backbone node X_{A} (center of the backbone cell containing A), through a single QKD link (an access link).
- The traffic is routed through the **optimal (less costly) path** over the backbone QKD network from X_{A} to X_{B} (QKD node closer to B).
- The traffic goes from X_{B} to B.

The routing rule defined above can be characterized as *geographical*, in the sense that it is driven by distance considerations. However, determining the optimal path in a given backbone network of arbitrary topology may not be a tractable problem. Even in standard networks, where the optimal path is the shortest one, an analytic computation of the average length/cost is not always possible. In the context of backbone nodes distributed as a Poisson point process, an alternative suboptimal routing policy, the so-called *Markov path*, has been proposed, and leads

to analytic computation of the average path length. In QKD networks, the cost is a nonlinear function of the length and some adjustments are required. We consider two different geometries for the backbone:

1. A square backbone QKD network (section 3.6.1), i.e. a regular structure where nodes and links form a regular graph of degree 4. In this case, finding the length of the shortest path between two nodes is trivial: backbone nodes X_A, X_B can be designated by cartesian coordinates (x_A, y_A), (x_B, y_B) and the shortest path length is simply $|x_A - x_B| + |y_A - y_B|$. Moreover, cost calculations are simplified using the fact that the links between two neighbor nodes of the backbone all have the same length.
2. A stochastic backbone network (section 3.6.2), where backbone nodes are distributed following a random point process and backbone cells are the corresponding Voronoï partition. For this stochastic backbone, we have used a routing technique called *Markov-path routing* for which, as previously established by Tchoumatchenko *et al* [24, 25], the average length of routes can be calculated. In the following, we will adapt these calculations to our cost function $C(\ell)$.

3.5.2. Generic derivation of the cost function for QKD backbone networks. For a QKD network with a backbone structure, we define $M = \{X_i\}$ as the point process of the network node distribution, and $\Pi = \{U_i\}$ as the point process of the network user distribution, with intensity density f. Each node X_i is connected to some nodes in its neighborhood and to the clients belonging to the associated cell D_i. In the following, we will assume that M is statistically independent of Π, and that the cells D_i are the Voronoï cells associated with M, that is

$$D_i = \left\{ x \ : \ \|x - X_i\| \leqslant \inf_{j \neq i} \|x - X_j\| \right\}. \tag{9}$$

In the case of the QKD backbone network, our routing policy allows us to calculate $C^{\text{pair}}(u, v; M)$, the QKD equipment cost associated with sending one unit of call between users u and v, over a network whose backbone nodes are described by the point process M:

$$C^{\text{pair}}(u, v; M) = \begin{cases} C(\|u - X_i\|) + C(\|v - X_i\|) \\ \qquad \text{if } u, v \in D_i, \\ C(\|u - X_i\|) + C(\|v - X_j\|) + C^{\text{hop}}(i, j; M) \\ \qquad \text{if } u \in D_i \text{ and } v \in D_j \text{ with } i \neq j, \end{cases}$$

where $C(\ell)$ is the cost spent to send a secret bit on a QKD link over a distance ℓ and $C^{\text{hop}}(i, j; M)$ is the cost to send a secret bit between the nodes X_i and X_j of the backbone for the given routing policy.

Given that the volume between each pair of users is V, the average total cost $\mathcal{C}$ of the QKD network then reads

$$\mathcal{C} = \mathcal{C}^{\text{QKD}} + \mathcal{C}^{\text{node}} = V \times \mathbb{E}\left[\sum_{k \neq l} C^{\text{pair}}(U_k, U_l; M) \right] + C_{\text{node}} N^2,$$

where N^2 is the average number of nodes of the backbone deployed in the domain D of size $L \times L$. Here $\mathbb{E}$ denotes the average cost over the spatial distributions of users and backbone nodes, that is over the realizations of Π and M. Since M and Π are supposed independently distributed, we may compute this average successively with respect to M and Π. The total cost, averaged only over Π, can be decomposed as follows:

$$\begin{aligned}
\mathbb{E}\left[\sum_{k\neq l} C^{\text{pair}}(U_k, U_l; M)\right] &= \int C^{\text{pair}}(u, v; M)\, f(u)\, f(v)\, \mathrm{d}u\, \mathrm{d}v \\
&= \sum_k \int_{D_k\times D_k} \{C(\|u - X_k\|) + C(\|v - X_k\|)\}\ f(u)\, f(v)\, \mathrm{d}u\, \mathrm{d}v \\
&\quad + \sum_{k\neq l} \int_{D_k\times D_l} \big\{C(\|u - X_k\|) + C(\|v - X_l\|) \\
&\quad + C^{\text{hop}}(k, l; M)\big\}\ f(u)\, f(v)\, \mathrm{d}u\, \mathrm{d}v \\
&= \sum_k \sum_l \int_{D_k\times D_l} \{C(\|u - X_k\|) + C(\|v - X_l\|)\}\ f(u)\, f(v)\, \mathrm{d}u\, \mathrm{d}v \\
&\quad + \sum_{k\neq l} \int_{D_k\times D_l} C^{\text{hop}}(k, l; M)\, f(u)\, f(v)\, \mathrm{d}u\, \mathrm{d}v.
\end{aligned}$$

As we can see from the last expression, the total cost $\mathcal{C}$ can be separated into three terms:

$$\mathcal{C} =: C^{\text{loc}} + C^{\text{bb}} + C^{\text{node}}, \tag{10}$$

where C^{loc} takes into account all connections from one client to the closest backbone node, C^{bb} all connections from one backbone node to another, and C^{node} is the cost of node equipment. The explicit models that we will study will allow us to compare the behavior of these different terms and thus to understand how QKD network backbone topologies can be optimized.

3.6. Cost calculations for two explicit quantum backbone models

3.6.1. Cost of the square backbone QKD network.

Network model. We consider, as a first simple example, the case of a QKD backbone network that has a perfectly regular topology, and for which the shortest path length between two backbone nodes is easily determined.

The architecture we consider is the following: users are distributed as previously over a large area D of size $L \times L$ and the backbone QKD network is a regular graph of degree 4, i.e. the backbone QKD nodes and links constitute a square network. The structure of the square backbone QKD network and the way a call is routed is summarized in figure 4. The free parameter with respect to which we will perform the cost optimization is the size of backbone cells α_{bb}. We will also make the assumption that the user density function f is uniform over D.

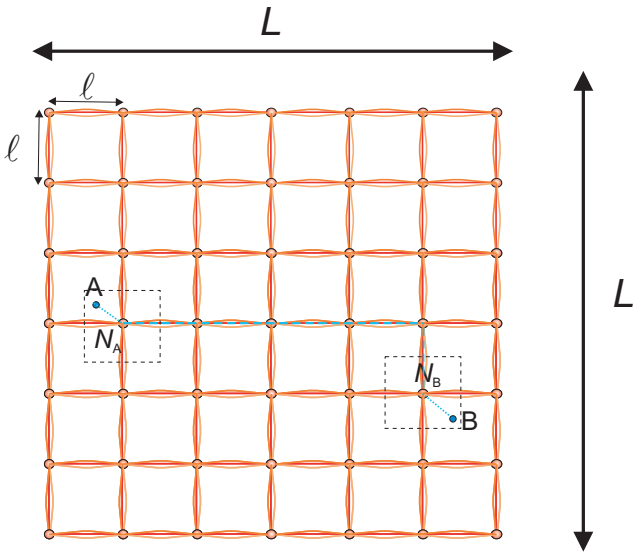

Figure 4. Structure of a 2D regular square backbone network: a regular array of cells of dimension α_{bb} spans a region of size $L \times L$. The user distribution is described by a random point process. In each cell, a central node collects all the local traffic. Every user in the cell is thus connected via a QKD link to the central node of its cell. On top of this array of cells, a backbone network connects first-neighbor QKD nodes with a QKD trunk. Traffic on the backbone network is routed through the shortest path. The dotted blue line describes the path followed for the communication between two users A and B (see text for more details).

Computation of C^{bb} for the square network. We set $X_k = k\alpha_{\mathrm{bb}}$ and $D_k = X_k + \alpha_{\mathrm{bb}}$ $[-1/2, 1/2]^2$ with $k \in \mathbb{Z}^2$ and, for all $k \neq l$,

$$C^{\mathrm{hop}}(k, l; M) = \|k - l\|_1 \, C(\alpha_{\mathrm{bb}}).$$

Here, $\|k - l\|_1$ corresponds to the number of hops between X_k and X_l and $C(\alpha_{\mathrm{bb}})$ to the per-bit cost of one hop.

Calling μ_i the average number of QKD users in a backbone cell i, we have:

$$C^{\mathrm{bb}} = V \sum_{k \neq l} \mu_k \mu_l \, C^{\mathrm{hop}}(k, l; M). \tag{11}$$

Hence,

$$C^{\mathrm{bb}} = V C(\alpha_{\mathrm{bb}}) \, \boldsymbol{\mu}^T \Gamma \boldsymbol{\mu},$$

where $\boldsymbol{\mu}$ is the column vector with entries μ_k, $k \in \mathbb{Z}^2$, and Γ is the Toeplitz array indexed on $\mathbb{Z}^2$ with entries $\Gamma_{k,l} = \|k - l\|_1$.

Since the density of users f is constant and equal to σ on its support D, where $D := \bigcup_{k \in \{0,\ldots,N-1\}^2} D_k$, μ_k is the same for all cells D_k: $\mu_k = \mu/N^2$, with N^2 denoting the total number

of backbone cells, and $\mu = (L/\alpha_u)^2$ the mean number of users over D (see equation (4)). Hence, we find

$$C^{bb} = VC(\alpha_{bb})\,\mu^2/N^4 \sum_{k,l\in\{0,\ldots,N-1\}^2} \|k-l\|_1.$$

Now, we compute

$$\begin{aligned}\sum_{k,l\in\{0,\ldots,N-1\}^2} \|k-l\|_1 &= \sum_{k_1,l_1=0}^{N-1}\sum_{k_2,l_2=0}^{N-1}\sum_{i=1}^{2}|k_i-l_i| \\ &= 2\sum_{k_1,l_1=0}^{N-1}\sum_{k_2,l_2=0}^{N-1}|k_1-l_1| = 2N^2\sum_{k,l=0}^{N-1}|k-l| \\ &= 4N^2\sum_{k=0}^{N-1}\sum_{l<k}|k-l| = 4N^2\sum_{k=0}^{N-1}\sum_{l<k}|k-l| \\ &\sim \frac{2}{3}N^5,\end{aligned}$$

where the asymptotic equivalence holds as $N \to \infty$. Using $N \sim L/\alpha_{bb}$ and equation (4), we obtain, as $N \to \infty$,

$$C^{bb} \sim V\frac{\mu^2}{N^4}C(\alpha_{bb})\frac{2}{3}N^5 = \frac{2}{3}\frac{C(\alpha_{bb}\alpha_u^4)}{\alpha_{bb}}L^5\,V = \frac{2}{3}\frac{C(\alpha_{bb})}{\alpha_{bb}}\mu^2 VL. \tag{12}$$

In the latter expression, we have four multiplicative terms:

1. $2/3$, a constant depending only on the dimension and the geometry of the backbone network (for a cube of dimension d, we could generalize our calculation and would find $d/3$);
2. $C(\alpha_{bb})/\alpha_{bb}$, a cost function depending only on the distance α_{bb} between the nodes of the backbone;
3. $\mu^2\,V$, the square of the mean number of users times the volume of call per pair of users, i.e. in our communication model, the total volume of the communications over which the total cost is computed;
4. L, the size of the support of f, that is of the domain where the users lie.

To understand better the derived expression for C^{bb}, it is interesting to compare it with C^{loc} and C^{node}. Indeed, we can show that $C^{loc} \simeq \mu^2\,\overline{C}$, where $\overline{C}$ stands for the per-bit cost function C averaged over one cell. In the case of the square network with $\alpha_{bb} \times \alpha_{bb}$ square cells, these cells are contained between two circles of radius $\alpha_{bb}/2$ and $\alpha_{bb}\sqrt{2}/2 < \alpha_{bb}$. Since C is an increasing function of distance we have $\overline{C} < C(\alpha_{bb})$, and we can thus derive the important following property: **In the limit of large networks**, i.e. **for** $L \gg \alpha_{bb}$, **the backbone cost is dominant over the local cost**. We will see in the following section that this property is preserved for a backbone with randomly positioned nodes and an appropriate routing policy. Furthermore, we will see that for large L, the backbone node equipment cost C^{node} is negligible. Therefore, to optimize the cost (equation (10)), we only need to minimize C^{bb}. Assuming a square regular backbone, this means choosing α_{bb} so as to minimize $C(\alpha_{bb})/\alpha_{bb}$, exactly as in the case of the linear chain QKD network model of section 3.2.

Hence, if we take $C(\ell) = \frac{C_{\mathrm{QKD}}}{R_0} \mathrm{e}^{\ell/\lambda_{\mathrm{QKD}}}$, the cost is minimized for

$$\alpha_{\mathrm{bb}}^{\mathrm{opt}} = \lambda_{\mathrm{QKD}}. \tag{13}$$

3.6.2. Cost calculation for a stochastic QBB with Markov-path routing. We now compute C^{loc} and C^{bb} in the case where the routing policy is the so called Markov path, as proposed in [25], where some general formulae are given for computing average costs in a general framework (see also [24]). The routing policy is defined as follows. First, all pairs of nodes whose cells share a common edge are connected. The corresponding graph is a Delaunay graph. Next, given two users A and B with respective positions u and v, we define a finite sequence of the nodes $X_{k_0}, X_{k_1}, \ldots, X_{k_n}$ in the successive cells encountered when drawing a line from u to v. This routing policy is illustrated in figure 3.

By definition, X_{k_0} and X_{k_n} are the centers of the cells containing u and v, respectively, and

$$\begin{aligned} C^{\mathrm{loc}} &= V \times \int_{D\times D} \mathbb{E}\left[C(\|u - X_{k_0}\|) + C(\|v - X_{k_n}\|)\right] f(u)\, f(v)\, \mathrm{d}u\, \mathrm{d}v \\ &= V\mu^2\kappa^{\mathrm{loc}}, \end{aligned} \tag{14}$$

where $\mu := \int f$ is the average total number of users and, by stationarity of the point process M,

$$\kappa^{\mathrm{loc}} = \mathbb{E}\left[C(\|u - X_{k_0}\|)\right] + \mathbb{E}\left[C(\|v - X_{k_n}\|)\right] = 2\mathbb{E}\left[C(\|X_0\|)\right]$$

with X_0 defined as the center of the cell containing the origin. Note that κ^{loc} denotes the average local cost per secret bit and per pair of users. If M is a Poisson point process with intensity $\alpha_{\mathrm{bb}}^{-2}$, we further have

$$\mathbb{P}(\|X_0\| > t) = \mathbb{P}(\#\{X_k \,:\, \|X_k\| \leqslant t\} = 0) = \exp(-\pi t^2 \alpha_{\mathrm{bb}}^{-2}),$$

and hence

$$\kappa^{\mathrm{loc}} = 4\pi\alpha_{\mathrm{bb}}^{-2} \int_{\mathbb{R}_+} C(t)\, t\, \exp(-\pi t^2 \alpha_{\mathrm{bb}}^{-2})\, \mathrm{d}t = 4\pi \int_{\mathbb{R}_+} C(\alpha_{\mathrm{bb}} u) u\, \exp(-\pi u^2)\, \mathrm{d}u. \tag{15}$$

For C^{bb}, we can write

$$C^{\mathrm{bb}} = V \times \int_{D\times D} \mathbb{E}\left[\sum_{i=1}^{n} C(\|X_{k_i} - X_{k_{i-1}}\|)\right] f(u)\, f(v)\, \mathrm{d}u\, \mathrm{d}v.$$

Applying [25, theorem 2] or the results (in particular theorem 2.41 and remark 2.4.2) in section 2.4 of [24] (as done in corollaries 2.5.1 and 2.5.2 in [24]), we obtain

$$\mathbb{E}\left[\sum_{i=1}^{n} C(\|X_{k_i} - X_{k_{i-1}}\|)\right] = \kappa^{\mathrm{bb}}\, \|u - v\|,$$

where

$$\kappa^{\mathrm{bb}} := 2\alpha_{\mathrm{bb}}^{-1} \int_{(r,\psi,\phi)\in\mathcal{A}} C\,(2\alpha_{\mathrm{bb}} r\ \sin(\{\psi-\phi\}/2))\ \{\cos(\phi)-\cos(\psi)\}\, r^2\, \mathrm{e}^{-\pi r^2}\, \mathrm{d}\psi\, \mathrm{d}\phi\, \mathrm{d}r, \tag{16}$$

and $\mathcal{A} = \mathbb{R}_+ \times \{(\psi,\phi) : 0 < |\phi| \leqslant \psi < \pi\}$. Finally, we find that

$$C^{\mathrm{bb}} = V \kappa^{\mathrm{bb}}\, \delta, \tag{17}$$

where δ is the average total distance between two different users defined in equation (7) and computed in equation (8), and κ^{bb} denotes the average backbone cost per secret bit and per length unit of the distance separating a pair of users.

From equations (10), (14) and (17), and observing that here the average total number of backbone cells $N^2 = (L/\alpha_{\mathrm{bb}})^2$, we find

$$\mathcal{C} =: C^{\mathrm{loc}} + C^{\mathrm{bb}} + \mathcal{C}^{\mathrm{node}} = V \times \left[\mu^2 \kappa^{\mathrm{loc}} + \delta \kappa^{\mathrm{bb}}\right] + C_{\mathrm{node}} (L/\alpha_{\mathrm{bb}})^2, \tag{18}$$

where μ^2 and δ are related to the spatial distribution of the users, and κ^{loc} and κ^{bb} are constants related to the geometry of the backbone and to the routing policy. For users uniformly distributed in a square of side length L with intensity α_{u}^{-2}, we have $\mu^2 \simeq (L/\alpha_{\mathrm{u}})^4$ and $\delta \simeq L^5/\alpha_{\mathrm{u}}^4$.

Using (15), (16), (18) and the above approximations of μ^2 and δ, we see that the total cost $\mathcal{C}$ only depends on L, α_{u} and α_{bb}. Now, for given α_{u} and L, we take α_{bb} so that $\mathcal{C}$ is minimized and examine which term in the right-hand side of (18) dominates the total cost $\mathcal{C}$ as $L \to \infty$ in this context. To this end, we first study each term separately. We let c denote a constant not depending on L, α_{bb} in the following reasoning. Observe that since C is convex and increasing, $C(\ell) \geqslant c \times \ell$. Using this in (15) and in (16), we get $C^{\mathrm{loc}} \geqslant c\, \alpha_{\mathrm{bb}} L^4$ and $C^{\mathrm{bb}} \geqslant c\, L^5$, respectively. Concerning the last term, we have $\mathcal{C}^{\mathrm{node}} \approx c\, L^2/\alpha_{\mathrm{bb}}^2$. It follows that at fixed L, $C^{\mathrm{loc}} \to \infty$ as $\alpha_{\mathrm{bb}} \to \infty$ and $\mathcal{C}^{\mathrm{node}} \to \infty$ as $\alpha_{\mathrm{bb}} \to 0$, from which we can deduce that the optimal α_{bb} stays away of 0 and ∞. Now, clearly, if α_{bb} stays away from 0 and ∞, the above bounds show that C^{bb} dominates as $L \to \infty$. Hence, for large L, the optimal intensity α_{bb} is the one that minimizes C^{bb} or, equivalently, κ^{bb}. To find this optimal intensity, the following result is useful for an exponential cost $C(\ell) = \frac{C_{\mathrm{QKD}}}{R_0} \mathrm{e}^{\ell/\lambda_{\mathrm{QKD}}}$:

Lemma 3.1 *Define κ^{bb} as in equation (16) with $C(\ell) = \frac{C_{\mathrm{QKD}}}{R_0} \mathrm{e}^{\ell/\lambda_{\mathrm{QKD}}}$. Then the following analytical formula holds:*

$$\kappa^{\mathrm{bb}} = C_{\mathrm{QKD}} R_0^{-1} \lambda_{\mathrm{QKD}}^{-1} \frac{4}{\pi} \left[\mathrm{e}^{\alpha_{\mathrm{bb}}^2/(\pi\lambda_{\mathrm{QKD}}^2)} \{1 + \mathrm{erf}(\alpha_{\mathrm{bb}}/(\sqrt{\pi}\lambda_{\mathrm{QKD}}))\} + \lambda_{\mathrm{QKD}}/\alpha_{\mathrm{bb}}\right],$$

where

$$\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x \mathrm{e}^{-t^2}\, \mathrm{d}t.$$

Proof. Let $s = \lambda_{\mathrm{QKD}}/\alpha_{\mathrm{bb}}$. We have

$$\int_{(r,\psi,\phi)\in\mathcal{A}} \exp\left(2s^{-1} r\ \sin(\{\psi-\phi\}/2)\right)\ \{\cos(\phi)-\cos(\psi)\}\, r^2\, \mathrm{e}^{-\pi r^2}\, \mathrm{d}\psi\, \mathrm{d}\phi\, \mathrm{d}r$$
$$= 8 \int_{v=0}^{\pi/2} \int_{r=0}^{\infty} \exp(2s^{-1} r\ \sin(v) - \pi r^2)\, r^2\ \sin(v)\, \mathrm{d}v\, \mathrm{d}r.$$

Integrating with respect to r yields

$$\kappa^{\mathrm{bb}} = C_{\mathrm{QKD}} R_0^{-1} \lambda_{\mathrm{QKD}}^{-1} \left[\frac{2}{\pi} + \frac{4s}{\pi} \int_{v=0}^{\pi/2} \sin(v)\{1 + 2\,\sin^2(v)/(\pi s^2)\} \times \exp(\sin^2(v)/(\pi s^2))(1 + \mathrm{erf}(\sin(v)/(\sqrt{\pi} s)\,\mathrm{d}v \right].$$

Further computations yield

$$\kappa^{\mathrm{bb}} = C_{\mathrm{QKD}} R_0^{-1} \lambda_{\mathrm{QKD}}^{-1} \frac{4}{\pi} \left[\mathrm{e}^{1/(\pi s^2)} \{1 + \mathrm{erf}(1/(s\sqrt{\pi}))\} + s \right],$$

which is the desired expression. □

Using lemma 3.1, the α_{bb} minimizing κ^{bb}, denoted as $\alpha_{\mathrm{bb}}^{\mathrm{opt}}$ below, can easily be calculated using a numerical procedure. We find

$$\alpha_{\mathrm{bb}}^{\mathrm{opt}} \approx 1.2490\,\lambda_{\mathrm{QKD}}. \tag{19}$$

This result should be compared with the result of equation (13), where the backbone geometry is deterministic and also characterized by the node intensity $1/\alpha_{\mathrm{bb}}^2$. These two results show that the choice of the backbone and routing policy does influence the optimal node intensity, albeit in a modest way.

3.7. From cost optimization results to QKD network planning

3.7.1. Matching QKD network topology with QKD links optimum working distance. The calculations in sections 3.6.1 and 3.6.2 point to one common result: it appears that, for large networks, the costs associated with the QKD devices that have to be deployed in backbone nodes to serve the demand are always dominant over the local costs, associated with the end connections between QKD users and backbone nodes.

Moreover, the optimization of backbone costs indicates that minimum cost will be reached when the typical distance between backbone nodes is of the order of λ_{QKD}, the scaling parameter of the curve $R(l)$.

These results lead to the following statements:

- When a QKD network deployment is planned, is seems optimal to choose the location of network nodes so that QKD links will be operated over distances comparable with the optimal distance ℓ^{opt}. As we have seen in our different models, ℓ^{opt} is always lower bounded by a prefactor times λ_{QKD}. Indeed, when the total cost of node equipment can be neglected compared with the cost of QKD devices, as it is the case for large networks, then the optimum distance ℓ^{opt} is indeed comparable with λ_{QKD}, which is roughly equal to 20 km. This indicates that current QKD technologies, for which D_{max} is already significantly larger than 20 km, are well suited for metropolitan operation. On the other hand, the typical distance between amplifiers, in optical wide area networks, is of the order of 80 km. If we wanted to deploy trusted QKD networks with the current generation of QKD devices, the QKD links would have to be operated close to their maximum distance, where the unit of secret bit rate becomes very expensive. Although technically already feasible, the

deployment of wide area QKD networks thus remains a challenge. We can, however, anticipate that this challenge will be overcome within the next years, as new generations of QKD protocols and devices, able to generate keys at higher rates, and with larger maximum distances are already being presented [26]–[28].

- The results on cost minimization that we have obtained could provide some helpful guidelines for QKD device developers: they may help promoting the idea that what will really matter, in the perspective of real network deployment, will be to focus on the optimization of their systems around typical network-optimum working distances. Optimizing QKD devices in this regime means reducing the cost of a unit bit rate at a *reasonable* distance, where the throughput of the QKD link is not considerably smaller than R_0. It will be of course always profitable to design QKD devices that can reach very long distances, but as discussed in [29], from a system development point of view it can be significantly different to optimize QKD devices to reach the longest possible distance $D_{\max}$, and to optimize them so that the cost of unit of bit rate is as low as possible, around the distance ℓ^{opt} minimizing network costs.

3.7.2. In which regime are backbones useful?. We would like now to use our calculation results to analyze in which regime QKD backbones become *economically interesting*, i.e. under which conditions it is interesting to introduce some hierarchy and resource mutualization in QKD networks, in order to decrease the total deployment cost.

In the previous sections, we have performed cost calculations that can be used to establish some quantitative comparisons between:

- The cost of a QKD network with no hierarchy as in the generalized linear chain QKD network, whose cost calculations have been performed in section 3.4.
- The cost of a QKD network with one level of hierarchy, which is the case of the square backbone QKD network studied in section 3.6.1.

Since these two cost calculations have been performed under the same assumptions regarding user distribution and traffic demand, we can use the results given in equations (6) and (12) to compare the total network deployment costs, respectively, for the generalized linear chain model and for a QKD network with a square backbone (for which we have seen that we could neglect the cost of the local access network).

The condition under which it will be more cost effective to deploy a quantum backbone than to connect all pair of users by 1D chains of QKD links can be described by the following inequality between the respective optimal costs:

$$\mathcal{C}_{\text{2D,chain}}^{\text{opt,chain}} \geqslant \mathcal{C}_{\text{2D,square}}^{\text{opt,square}} \Leftrightarrow \left(V\, C(\ell^{\text{opt}})/\ell^{\text{opt}} + C_{\text{node}}/\ell^{\text{opt}}\right)\gamma\sigma^2 L^5 \geqslant \frac{2}{3}\, C(\alpha_{\text{bb}}^{\text{opt}})/\alpha_{\text{bb}}^{\text{opt}}\, \sigma^2 L^5\, V + C_{\text{node}}\, L^2/\alpha_{\text{bb}}^{\text{opt}^2}. \tag{20}$$

The above equation is not very convenient to handle because in general $\alpha_{\text{bb}}^{\text{opt}} \neq \ell^{\text{opt}}$. However,

$$\mathcal{C}_{\text{2D,chain}}^{\text{opt,chain}} \geqslant \mathcal{C}_{\text{2D,square}}^{\text{opt,square}} \Rightarrow \mathcal{C}_{\text{2D,chain}}^{\text{opt,square}} \geqslant \mathcal{C}_{\text{2D,square}}^{\text{opt,square}}. \tag{21}$$

Thus, we can derive a necessary condition under which the deployment of a backbone for a QKD network is a better solution than a design that would solely rely on the generalized linear chain of QKD links to transport the traffic:

$$C_{\mathrm{2D,chain}}^{\mathrm{opt,square}} \geqslant C_{\mathrm{2D,square}}^{\mathrm{opt,square}} \Leftrightarrow C_{\mathrm{node}}\,(\sigma^2 L^3 \alpha_{\mathrm{bb}}^{\mathrm{opt}}\,\gamma - 1) \geqslant C(\alpha_{\mathrm{bb}}^{\mathrm{opt}}) V\,\sigma^2 L^3 \alpha_{\mathrm{bb}}^{\mathrm{opt}} \left(\frac{2}{3} - \gamma\right)$$

$$\Leftrightarrow C_{\mathrm{node}}\,(\sigma^2/\sigma^{*2} - 1) \geqslant C(\alpha_{\mathrm{bb}}^{\mathrm{opt}})\,V\,\sigma^2/\sigma^{*2} \left(\frac{2}{3\gamma} - 1\right) \tag{22}$$

with $\sigma^* = 1/\sqrt{L^3 \alpha_{\mathrm{bb}}^{\mathrm{opt}}\,\gamma}$.

Keeping in mind that $\frac{2}{3\gamma} - 1$ is a positive number, we can use the last inequality to make the following observations:

- First, it appears that, if the user density σ is smaller than σ^*, which we can qualify as a *critical user density*, then equation (22) can never be verified. This means that below σ^* it will never be interesting to deploy a backbone. This result has a clear interpretation: backbone infrastructures can only be interesting in the case where sharing resources offers a cost reduction. And the incentive to share a backbone infrastructure can only exist if there are enough users. The minimum total number of users required to have a cost incentive toward backbone deployment is $\sigma^* L^2 = \sqrt{L/(\gamma \alpha_{\mathrm{bb}}^{\mathrm{opt}})}$.
- In the case that σ is larger than the critical user density σ^*, we enter a regime where there will be an incentive to deploy a quantum backbone essentially if the cost of a node C_{node} dominates over the cost of QKD link equipment to be deployed, which scales as $C(\alpha_{\mathrm{bb}}^{\mathrm{opt}})V$. This also has a clear interpretation: if we take the extreme case where building a node (and installing node equipment inside it) is zero, we can foresee that there will be no incentive to build a backbone: it will always be cheaper to deploy direct chains between each pair of users. The motivation to build a backbone arises when efforts associated with opening a QKD node are important. This will of course be the case if QKD node equipment is expensive, as we can see from equation (22), but it is also intuitive that, in case significant efforts are required to build new QKD nodes, mutualization of nodes through a backbone structure will be a cost effective solution.

4. Conclusion and perspectives

In this paper, we performed a topological analysis of QKD networks with trusted repeater nodes. In particular, under specific assumptions on the user and node distributions as well as the call traffic and routing in such networks, we derived cost functions for different network architectures. We first considered a linear chain network as a basic model that served the purpose of illustrating the main techniques and ideas that we used, and then moved on to more advanced network configurations that were in some cases enhanced with a backbone structure. Using cost minimization arguments, we obtained results on the optimal working points of QKD links and spatial distribution of QKD nodes, and examined the importance of introducing hierarchy into QKD networks.

Our results indicate that, in the context of QKD networks, it is more cost-effective and therefore advantageous to operate individual QKD links at their optimal working point, which is in general significantly shorter than the maximum span of such links. This conclusion motivates research into new experimental compromises in practical QKD systems, and can be illustrated by considering examples of such systems where the characteristics of either a hardware component (for example a single-photon detector) or a software algorithm (for example a reconciliation code) can be experimentally manipulated as a function of distance [29].

In general, it is clear that, as the realization of more and more advanced QKD networks approaches the realm of actual deployment, it becomes necessary to orient the research on QKD devices and links toward cost-related directions, and extend the techniques we have presented here to more sophisticated network technologies and architectures.

Acknowledgments

We acknowledge financial support from the Integrated European Project SECOQC (grant no. IST-2002-506813). RA and ED acknowledge financial support from the French National Research Agency Projects PROSPIQ (ANR-06-NANO-041-05) and SEQURE (ANR-07-SESU-011-01). NL acknowledges support from the NSERC Innovation Platform QuantumWorks, an NSERC Discovery Grant and the Ontario Centers of Excellence.

References

[1] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 *J. Cryptol.* **5** 3
[2] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[3] Dušek M, Lütkenhaus N and Hendrych M 2006 *Progress in Optics* vol 49 ed E Wolf (Amsterdam: Elsevier) p 381
[4] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2008 arXiv:0802.4155 [quant-ph]
[5] http://www.idquantique.com
http://www.smartquantum.com
http://www.magiqtech.com
[6] Elliott C 2002 *New J. Phys.* **4** 46
[7] Elliott C *et al* 2005 arXiv:quant-ph/0503058
[8] http://www.secoqc.net
[9] Salvail L, Peev M, Diamanti E, Alléaume R, Lütkenhaus N and Länger T 2009 *J. Comput. Secur.* at press (arXiv:0904.4072v1 [quant-ph])
[10] Briegel H-J, Dür W, Cirac J I and Zoller P 1998 *Phys. Rev. Lett.* **89** 5932
[11] Collins D, Gisin N and de Riedmatten H 2005 *J. Mod. Opt.* **52** 735
[12] Dianati M, Alléaume R, Gagnaire M and Shen X 2008 *Secur. Commun. Netw.* **1** 57
[13] Peev M *et al* 2009 *New J. Phys.* **11** 075001
[14] Yuan Z L, Kardynal B E, Sharpe A W and Shields A J 2007 *Appl. Phys. Lett.* **91** 041114
[15] Diamanti E, Takesue H, Honjo T, Inoue K and Yamamoto Y 2005 *Phys. Rev.* A **72** 052311
[16] Hadfield R H, Stevens M J, Gruber S S, Miller A J, Schwall R E, Mirin R P and Nam S-W 2005 *Opt. Express* **13** 10846
[17] Ma L, Chang T, Mink A, Slattery O, Hershman B and Tang X 2007 *IEEE Commun. Lett.* **11** 1019
[18] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238

[19] Lodewyck J *et al* 2007 *Phys. Rev.* A **76** 042305
[20] Zbinden H, Bechmann-Pasquinucci H, Gisin N and Ribordy G 1998 *Appl. Phys.* B **67** 743
[21] Kosaka H, Tomita A, Nambu Y, Kimura T and Nakamura K 2003 *IEEE Electron. Lett.* **39** 1199
[22] Korneev A *et al* 2007 *IEEE J. Sel. Top. Quantum Electron.* **13** 994
[23] Baccelli F, Klein M, Lebourges M and Zuyev S 1997 *Telecommun. Syst.* **7** 207
[24] Tchoumatchenko K 1999 *PhD Thesis* Université de Nice, Sophia Antipolis
[25] Baccelli F, Tchoumatchenko K and Zuyev S 2000 *Adv. Appl. Probab.* **32** 1
[26] Stucki D *et al* 2008 arXiv:0809.5264 [quant-ph]
[27] Leverrier A and Grangier P 2008 arXiv:0812.4246 [quant-ph]
[28] Dixon A R, Yuan Z L, Dynes J F, Sharpe W and Shields A J 2008 arXiv:0810.1069 [quant-ph]
[29] Alléaume R, Roueff F, Diamanti E and Lütkenhaus N 2009 Long-distance quantum key distribution networks: cost calculations and optimal working points of individual links, in preparation