Development of a Global Network for Secure Communication based on Quantum Cryptography
www.secoqc.net

D-NET-04
Topology and cost optimization of the QKD network*

Project Document Number: D-NET-04
Deliverable type: Report
Version : 1.0
Status: Delivered
Document Date: 8th May 2006
Security class RE: restricted to a group specified by the consortium (including the Commission Services)
Authors: Romain ALLÉAUME[†], Franşois ROUEFF[†], Gilles ZEMOR[†], Gérard COHEN[†], Norbert LÜTKENHAUS[‡].

[†] Ecole Nationale Supérieure des Télécommunications, Paris, France.
[‡] University of Erlangen, Germany & IQC, Waterloo, Canada.

**This document is delivered in replacement of what was originally planned to be D-NET-04: "Performance of the QKD network and protocol optimization", please read the Foreword for explanations.*

Contents

Introduction

Foreword - Justification of deviation

The organization and the ideas within the Secoqc project have considerably progressed over the time period spanning from September to December 2005. The subproject NET has contributed to this evolution and the work performed within the subproject has also evolved in consequence. A general description of the Secoqc network, focusing on the concepts and on a coarse logical specification of the network are indeed building has been proposed [3]. From it and from subsequent discussions and meetings, a clearer understanding together with a wider agreement regarding the "network of secrets idea"has emerged.

NET has also spent an important effort on the specification of a logical and material interface between the QKD devices and the network higher layers. This work has led to the technical reports and deliverables related to Q3P(TR-NET-02 and D-NET-03). In parallel, the specification of a protocol stack for higher layers of the QKD network, called QSLS, has also begun (TR-NET-03 and D-NET-03). It however appeared that the notions linked to the "performance of the QKD network and protocol optimization", notions that were planned to be the subject of the deliverable D-NET-04, cannot be tackled seriously at this stage. A precise specification and verification of the different network protocols has to be available in the first place and ENST (partner 40) is currently focusing on this goal for NET. Simulations and performance evaluation are thus tasks that will be performed later in NET.

Event though the scope of this document is not protocol optimization its content is however not disconnected from what had been planned to be tackled in D-NET-04 : considering the QKD network from a topological perspective will lead us to define metrics related to the QKD network performance, and to look for network topologies that are optimum under these metrics. As we will see, investigating and characterizing the possible network topologies is a useful line of research to understand how the different network parameters influence on its performance. As a consequence it will also be a useful guide for the future work within SECOQC in order to further specify the structure and the protocols of the network.

Summary

The purpose of this document is to present the results and references gathered during a work done by ENST in collaboration with Norbert Lütkenhaus in order to answer to an initial question: what are the elements that should drive the design of a QKD network, what will it mean in terms of topology ?

This question was raised during the discussions that lead to the criteria for the QBB

We have focused our attention on the consequences of the typical Rate versus Distance behavior of a QKD link and on the cost functions that could be derived from this curve, for different QKD network topologies.

We will begin this document by introducing some background elements on the metrics in use in the network literature to characterize topologies and give an overview of the methods that are relevant in the cases we have considered. We will then draw our attention on QKD links modelization. We will expose our notations and explain how one can derive a cost function for QKD links. This QKD link cost function will be the basis of the calculations performed in the last chapter, whose objective is to study the the behavior of the cost function of entire QKD networks, for different topologies and traffic demands.

Chapter 1

Topology and classical networks : general background

The different problems related to the topology of communication networks have attracted considerable interest in the research literature. As previously stated [3, 4], the "network" part of the SECOQC QKD network, is essentially a classical object whose task is to perform long-distance, highly secure key distribution. It is therefore not surprising that when one is to design the SECOQC network, many of the questions that arise happen to be standard problems in communication networks. Based on this observation, we present here an overview of methods and results that are actively studied in the research literature and that we find of particular interest in the perspective of designing a QKD network.

1.1 Introduction: why topology matters ?

Describing a network can be done at many different levels and addressed through many different questions: what are the modular elements composing the network ? what logical structure ? what protocols ? what services are provided by the network ? to what kind of users ? ... These questions are all of high importance and need to be answered to build something that will eventually "work". However, even after getting answers to these questions, one would still be missing a general view of the "object" we are talking about.

Indeed, probably more than the other features evoked above, the description of the network topology can offer a very comprehensive grasp on the general properties of a network. It is also important to keep in mind how strategic the knowledge of a given network topology is: without it, one cannot, for example, answer to the questions we evoked in the beginning of this section.

Placing ourselves in the perspective folllowed within SECOQC, we can try to give an overview on the network performance measures that are directly connected to the topological structure we will have for the QKD network.

- Cost of the network.
  Even though cost is by itself not a performance measure, it is of course one -if not the most - important parameter when making a decision regarding network architecture or planning. Since topology is related to the amount of resources deployed, there is a direct relation between the global cost of a network infrastructure and its topology. As far as performance measures are concerned, cost (or more generally "the amount

of resources") is a parameter that has always to be taken into account. Indeed all performance measures shall be considered as "performance measure of the network, given a cost constraints of ..." i.e always take a metric related to the cost of the network as a parameter.

- Network capacity.
  What are the achievable rates that can be supported over the network ? To address this question, specific topological characteristics of the network, such as the connectivity or the diameter of the underlying graph play a key role.

- Achievable security
  As first explained in [1] path redundancy can be exploited to enhance the security of a QKD-based network by allowing a given session key to be established by the XOR of multiple intermediate keys, each one being established over a disjoint path in the QKD network.

- Resilience of the network - tolerance to errors, failures or attacks.
  Topological properties of the network, such as the variation of its connectivity when some of its nodes are removed, can also characterize the fault tolerance or the attack tolerance of a network [5, 10]. Indeed, as we shall discuss in chapter 2, since the SECOQC QKD network is targeting very high security, a special effort will be needed at the level of the QKD network topological design to ensure a high tolerance to attacks.

- Protocol performances.
  A communication network is by definition a system where protocols and algorithms are implemented over distributed systems. This is for example the case with path establishment protocols, or path restoration protocols. The performance of these protocols is largely determined by the distribution of the ressources over the network, i.e by the network topology.

- Scalability - Extendibility.
  Depending on the ways nodes are connected with each other, the difficulty of extending the network while maintaining its structure can greatly vary. For instance tree structures are typically easier to extend that highly connected structures.

As we can infer from the list above, it is usually not too difficult to define how a given performance measure can qualitatively vary with the topological properties of a network. The most meaningful analysis are however usually linked to the cross-optimizion of several performance measures and to the possibility of establishing quantitative comparisons between possible solutions. To perform this kind of studies, it is necessary to limit the range of investigation to some well-chosen quantitative properties of the network, i.e to refer to some metrics and to some generic topological properties, topics that are tackled in the next sections.

1.2 Metrics

1.2.1 Structural metrics

Structural metrics are intrinsic properties of the network graph i.e independent of how the network is used. The network graph G can be represented by two sets: the set of nodes called V (for "vertices") and the set of links called E (for "edges"). We will review here

some of the fundamental structural metrics that are useful to characterize the topology of a graph, choosing the metrics that are the most often used in the literature [5].

Number of nodes n

This metric is also sometimes called the *order* of the network. It is an indication of the network size. Large networks typically consists of networks for which $n \geq 1000$.

Diameter $\mathcal{D}$

The diameter of a network is the longest distance between a pair of nodes within the network. The unit used to measure the network diameter can be either the number of hops or the total link length. In case of a fiber optics network, the length diameter is usually a good indicator of the cost of the fiber infrastructure.

Average inter-nodal distance $\overline{\mathcal{D}}$

Rather than the diameter, the average inter-nodal distance is often considered. It is defined as:

$$\overline{\mathcal{D}} = \frac{1}{n^2} \sum_{v_i, v_j \in V} d(v_i, v_j) \tag{1.1}$$

where $d(v_i, v_j)$ stands for the euclidean distance between node v_i and node v_j.

Degree Δ

The degree of a node i, Δ_i is the number of links attached to this node. As an extension, the degree of a network is the maximum number of links attached to a node within the network topology:

$$\Delta = max_{\{i \in 1..n\}} \Delta_i$$

The topology will be said to be *regular* is all nodes have the same degree, as it is the case in a square network (see 3.5).

Number of links m

This metric corresponds to the cardinal of the set of links E: we have $m \equiv |E|$ and we have, as a consequence, a direct relation between the degree of the nodes and the number of links:$m = \frac{1}{2} \sum_{i=1}^{n} \Delta_i$.

Relationship between the number of nodes, the degree and diameter of a graph

For a fixed number of nodes n, the degree and the diameter evolve in opposite directions: dense networks (low diameter) tend to have a high degree if n is fixed. There is a bound, called Moore's bound $n_{\text{Moore}}(\Delta, \mathcal{D})$ which represents an upper bound for the order of a topology with given degree and diameter:

$$n_{\text{Moore}}(\Delta, \mathcal{D}) = 1 + \Delta \sum_{i=0}^{\mathcal{D}-1} (\Delta - 1)^i \tag{1.2}$$

Fault tolerance

Fault tolerance is linked to the number of distinct paths between each pair of source / destination nodes in the network. High fault tolerance is desirable for core networks, designed to support high rates as it will be the case for the backbone QKD network. Different quantitative measures can be proposed to assess fault tolerance:

- The maximum number of links that can be removed from the network without disconnection.
- The strong fault tolerance criteria: a network G is said to be fault tolerance if, when removing at most $\Delta - 2$ nodes within the network, each remaining pair of nodes v_i, v_j is still connected by $min\{\Delta_f(v_i), \Delta_f(v_j)\}$ disjoint paths, where $\Delta_f(v_i)$ and $\Delta_f(v_j)$ are the numbers of neighbors of the nodes v_i and v_j respectively.

1.2.2 Functional metrics

Functional metrics take into account the traffic engineering within the network, i.e information such as the flows on the links, routing schemes, node functionality etc. and allow to characterize quantitatively the network performance. As explained in [7], functional metrics together with structural metrics are interrelated and it is usually possible to consider a small number of such parameters to assess the performance of a given topology.

The traffic weighted metrics

Under a given traffic model, one can define the distance probability distribution of traffic demands, i.e the average probability $P(d)$ that a randomly chosen unit of communication demand corresponds to a distance origin to destination of d (in fiber length or number of hops). We can thus defined the weighted average distance $D_{weighted}$ as:

$$D_{weighted} = \sum_{d=d_{min}}^{\mathcal{D}} dP(d) \tag{1.3}$$

Total external traffic - Capacity

A measure of the network capacity is the total load that can be supported by the network, while ensuring a minimum quality of service (like an upper bound on the probability of call blockage). The total external traffic is a quantity that corresponds to the maximum traffic load that can be supported by the network. It is obtained by fixing the network topology, routing policy and a minimum quality of service and optimizing the total load (as a sum of origin-destination flows) over all the possible matrices of traffic demand flows between any two pairs of nodes in the network.

Flow number

The flow number is a functional metric that is used in WDM optical networks to quantify the number of wavelength needed to connect any pair of nodes. To derive it, one supposes that the flow traffic demand is constant, equal to one for each pair of node. We then define the ensembles $R_1..R_k$ as the sets defining all the origin-destination paths. Each one of these k sets can be seen as resulting from a routing policy. The flow number can thus be computed as the minimum over k of the maximum link load (over all the links within the network).

With the previous definition, the flow number depends only on the topology of the network, at the difference of the *network load* that would be the maximum link load for a given specific routing policy and matrix of traffic demand.

1.3 Connecting network optimization and network modelling

The classic approach to network analysis can be decomposed approximatively in the following steps:

- Choose a way to model the network resources. For example queuing systems associated with nodes and bandwith-limited links connecting nodes, operating with defined typical error rate and delays.
- Choose a model for the traffic over the network.
- Choose a set of criterias (metric) to estimate the behavior of the network under the studied traffic demand. Study the relations between the value taken by these metrics, the network model and the traffic.
- Dimension the network to reach some goals, like maximum delays, maximum probability of blocked call, or minimum redundancy.

1.3.1 The different network modelling approaches

Choosing a network model usually means making a compromise between the objective of capturing as much as possible its behavior and the objective of being able to make decisions based on model results, which implies solving the equations that were obtained.

When it comes to the network topology, the simplest solution is to consider simple geometries based on regular structures such as trees or rings in one dimension or regular bidimensional lattices. We will opt for such an approach in this document.

The problem with regular networks is that they may introduce some systematic bias in the optimization results, as explained in [8]. Working on random structures, based on stochastic point processes allows to overcome this difficulty and we have also investigated this aspect in our models for the QKD backbone network. However, due to the simplicity of the cost functions we have considered so far, it has appeared that we are not gaining much insight with the random graph approach.

1.3.2 Modelling network traffic: different time scales lead to different problems

Modelling the traffic in indeed a central issue as it strongly influences the type of metric that can be optimized. Indeed, depending on the time scales on which the traffic variation are considered, the standard network modelling tools and goals will be different:

- When averaged over long times (like years), the traffic can be treated as a set of continuous streams and modeled by a flow matrix. In this perspective, all dynamic effects such as delays, collisions in media access control will be neglected. Flow models are used in particular in what is called strategic planning, i.e high-level modelling, occuring potentially much earlier than deployment.

- Dynamic models must be established to understand the origin of delays and congestion in the system that may occur even when the average traffic does not exceed the capacity. In this perspective, one has to choose an appropriate time-scale to capture the burstiness of the traffic together with the non-stationnar behavior of queues. Such dynamical modelling is typically done to dimension an already deployed network.

Since QKD networks are far from being commonly deployed in real infrastructures, it seems natural to adopt flow traffic models in this case. We will even go further in the simplification by considering essentially "flat" traffic demands, i.e with equal flow between any pair of nodes.

Chapter 2

Modeling the QKD network

2.1 Introduction

At a very generic level, the QKD network can be described as a set of QKD links connecting distant QKD nodes whose function is to perform symmetric key establishment, with unconditional security between any pair of its QKD nodes.

A QKD network is a structure dedicated to key distribution whose physical layer is made of QKD links. As in any communication network, the characteristics of its physical layer plays a major role when it comes to topological design. We will discuss this point in the first section of this chapter.

Besides the use of QKD links, there are other specific requirements that we have agreed upon and some choices we have made within SECOQC, . We will review these aspects in the second section of this chapter.

Finally, we will discuss what can be the objectives of performing topological optimization in the case of the SECOQC QKD network.

2.2 Characteristics of a QKD network

2.2.1 General definitions

Definition of a QKD link

A QKD link is defined as the combination of a quantum and a classical channel together with the equipment that has to be deployed in the 2 QKD nodes placed on both endpoints of these channels.

Definition of a QKD node

A QKD node is a secure location able to host the equipment needed to run one of the endpoint of a QKD link.

The QKD network as an undirected graph

Although it will interesting to consider the possibility to use different types of QKD links or different QKD nodes in future work, we will here restrict ourselves to the case where all QKD links have the same characteristics. This simplification allows to make a natural description of the QKD network as an undirected graph $G = (V, E)$ where V stands for the

set of vertices, that we will also call QKD nodes and E is the set of under edges (consisting of QKD links placed between QKD nodes). This graph is said to be "undirected" because of the nature of quantum key establishment over a QKD link is intrinsically symmetric between the two nodes directly connected nodes.

2.2.2 Cost functions

Cost of a QKD link

If we strictly refer to the definition above, the cost of a QKD link should take into account a rather complex addition of different costs, some being linked to capital expenditures (CAPEX) while others are linked to operational expenditures (OPEX).

1. Cost of the QKD devices on both ends (CAPEX and OPEX).
2. Cost of the quantum and classical channel: Here we can distinguish the renting / amortizing cost of the links (OPEX) and the installation cost (CAPEX).

Cost of a QKD node

We can here also distinguish installation costs from operational costs. The latter is however extremely difficult to define since it is basically a function of how physically secure this location is, a notion that cannot be quantified easily.

2.2.3 Simplifying assumptions and justifications

Cost of a QKD link

Our main simplifying assumption will be to directly relate the cost of a QKD link, of a given capacity, to the cost of the QKD devices that need to be deployed to reach this link capacity[1].

Our assumption can be justified if we consider that we want to evaluate only the deployment cost of QKD on an existing infrastructure, where all nodes and channels are already installed and their associated operational costs not part of the calculation. We will also make the assumption that many possible solutions (locations) are available, hence that there are many choices on the possible topology of the QKD network.

We will call C_{QKD} the cost of the QKD devices needed to equip one QKD link. The associated capacity $R(l)$ (rate of secret bits) depends of the length of the link l. We will take the following definition:

$$C(l) \equiv C_{QKD}/R(l) \tag{2.1}$$

Because of our simplifying assumption, $C(l)$ corresponds to the cost of one unit of capacity over a QKD link of length l.

Cost of a QKD node

Following the logic leading to the definition of the cost of a QKD link, the cost of a QKD node corresponds to the expenses needed to equip one available location of the network and make it a "trusted QKD node". We will call C_n the cost of a QKD node.

[1] There is another implicit simplifying assumption in what we just wrote, namely that installation cost can be averaged over time and be integrated in the operational costs.

As we explained, this cost is very difficult to evaluation and we will often not take it into account. This simplification is equivalent of making the assumption that rates exchanged on the network are extremely high and thus that the cost of links dominate over the cost of nodes.

It is however very likely that setting up a QKD node can be something quite expensive, and the previous assumption may not always be correct. We will discuss its validity in 3.1.3.

2.2.4 Modeling the performance of a single QKD link

The performance of a QKD link can essentially be captured through two indicators :

1. The per-bit cost of secret key rate, as a function of distance.
2. The reliability of the link, that is related to its probability of failure.

Since all the results presented in this document have been derived in the limit of traffic models based on flows, where all dynamical effects are averaged over time, we don't need yet reliability to appear in our models. We thus have based our work solely on the per-bit cost function of link capacity and its evolution as a function of distance.

Secret bit rate versus distance

Difficulty to establish comparisons...

The secret bit rate performance $R(l)$ of a given QKD link of length l varies from system to system. This is of course also the case of C_{QKD}, the cost of a pair of QKD devices, a value that is difficult to assess. The per-bit cost of a unit of secret rate:

$$C(l) = C_{QKD}/R(l)$$

is thus also element difficult to evaluate and as a consequence for which it is difficult to establish comparison between systems. Comparisons are moreover all the more difficult to establish that calculated values are greatly influenced by the security model used in the calculations (see deliverable D-QIT-02 [13] for an extensive account on the information regarding the performance of the systems developed within SECOQC).

... but a general behavior can be defined

As shown on figure figure 2.1, the typical curve [2], describing the variation with distance of the logarithm of the mean rate of secret bit establishment can be essentially separated in two parts: what we will call the **linear** part is the region where the rate of secret key establishment varies as a given power of the propagation attenuation, followed by an **exponential drop-off** of the secret key rate at larger distances, when the error rate rapidly increases due to the growing contribution of detection dark counts [3].

One basically need only three parameters to characterize the shape of the secret bit rate versus distance functions $R(l)$:

[2] this curve is a log plot of the Rate versus Attenuation curve : the distance here on the x-axis scales varies logarithmically with respect to attenuation, while the Rate is explicitly plotted in log scale

[3] If for short distances, the rate of quantum communications causes a saturation of the detection setup, then a third part must be added in the curve, taking this saturation of the mean rate of secret key establishment into account. We will not consider this case here.

1. The secret bit rate at zero distance, R_0.
2. The scaling parameter λ_{QKD} in the linear regions such that $R(l) = R_0\, e^{-l/\lambda_{QKD}}$.
3. The maximum distance D_{max}.

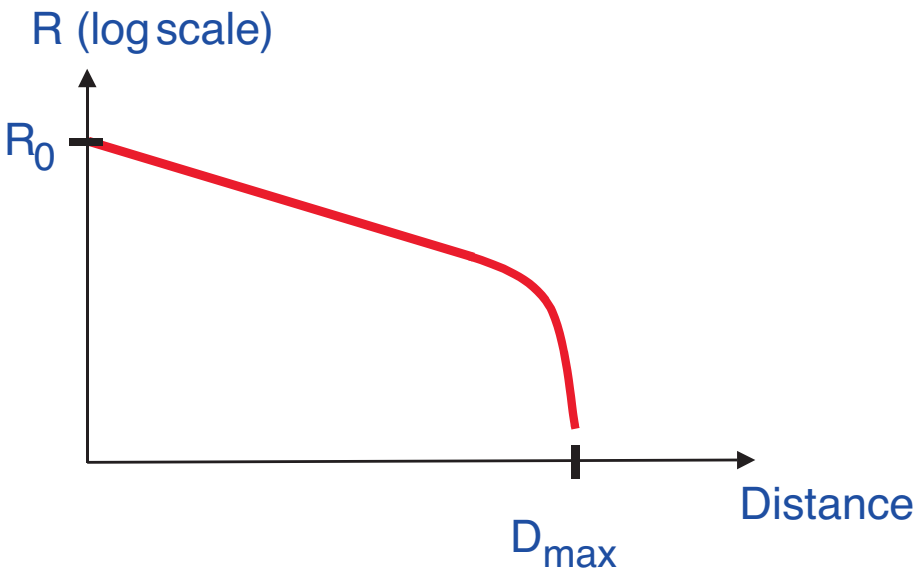

Figure 2.1: Typical profile of the Rate versus Distance curve for a single QKD link.

2.2.5 The scaling parameter λ_{QKD}

Losses on optical fibers are usually quantified by the value of α, the attenuation coefficient in dB/km. Neglecting irregularities and connector losses, $\eta(l)$, the attenuation on a fiber of length l, is thus given by:

$$\eta(l) = 10^{-\alpha l/10} \tag{2.2}$$

In the linear part of the curve displayed on figure 2.1, the rate $R(l)$ varies as a given power r of the attenuation :

$$R(l) = R_0\, \eta(l)^r \tag{2.3}$$

The value of r is mainly related to the security proof that can be applied to the experimental system, as explained in [13]. While the decoy state method allows to take $r = 1$, systems relying on weak coherent pulses vulnerable to PNS attack have to take $k = 2$ and their rate thus drop faster with distance. It is not the subject of this deliverable to dispute what value of r must be taken and we refer to the work of the QIT subproject for detailed answers to this question. On the contrary, we can notice that a global scaling parameter can be defined for the QKD rate, i.e a typical length λ_{QKD} such that:

$$R(l) = R_0 e^{-l/\lambda_{QKD}} \tag{2.4}$$

We can express λ_{QKD} in terms of the attenuation coefficient and the parameter k:

$$\lambda_{QKD} = l/ln(R_0/R(l)) = \frac{10}{\alpha ln(10) r} \tag{2.5}$$

Numerical evaluation
For $\alpha = 0.25\,dB/km$ and $r = 1$ we have : $\lambda_{QKD} \simeq 17km$.

2.2.6 Maximum distance D_{max} and detector performance

As we can see from equation 2.2, attenuation scales exponentially with distance and the linear regime corresponds to the situation described by equation 2.3, when the logarithm of the rate scales linearly with distance.

The assumption behind linearity is that the amount of generated key varies linearly with the rate of detected signal on Bob side. The domain of validity of this assumption ends when the error rate becomes too high, i.e when p_s the probability to detect some signal sent on the quantum channel becomes comparable to the probability to detect noise. Since most of the noise in a QKD set up comes from the dark counts of the detectors, we have the following condition around D_{max}:

$$p_s \simeq p_d \tag{2.6}$$

where p_d stands for the probability to get a dark count in a detection timeslot.

The probability to detect a signal in a given timeslot is conditioned by two things:

1. The signal photon must have been transmitted through the fiber (and not lost during propagation).
2. It must be *detected*, which occurs with probability η_d (efficiency of the detector).

If we combine these two conditions with the fact that they occur for $l \simeq D_{max}$ we have:

$$ps = e^{-D_{max}/\lambda_{QKD}} \times \eta_d \simeq p_d \tag{2.7}$$

i.e

$$D_{max} \simeq \lambda_{QKD}\, ln(\eta_d/p_d) \tag{2.8}$$

Practically, when working with InGaAs SPADs at 1550 nm, the ratio η_d/p_d is optimized by working on the different external parameters of the detector: temperature, gate voltage, timeslot duration ... The best published performances [14, 15] relate values of the dark count $p_d \simeq 10^{-6}\, to\, 10^{-7}$, for a detection efficiency η_d around 10%. We thus have

$$D_{max} \simeq (5\, to\, 6)\lambda_{QKD} \tag{2.9}$$

2.2.7 About the "linearity assumption" on the cost functions

In most of our derivations, we will assume a purely linear dependency of $log(R(l))$ with l, i.e not take into account the saturation happening around D_{max}. If we look at QKD links from a telecom point of view, it seems clear that it is highly desirable to operate the links in the **linear** part of their characteristics, i.e on spanning distances smaller than D_{max}, in order to avoid the exponential drop-off of performance around $Dmax$. However, such a requirement should not be imposed beforehand in our topological optimization: indeed, for some special topology and demand matrix, it may happen that the minimum cost of operation of the network is reached with QKD links stretching over distances close to D_{max} [4]. More generally, the "linearity assumption" we make must be checked a posteriori before any solution is validated.

[4] Even if a solution with QKD links operated in the D_{max} region might be mathematically the optimum one, it will surely be quite a bad solution in practice: the resulting mean cost for a bit exchange will be very high, as well as the latency of the key distribution network. In such cases, we would be forced to question whether or not it makes sense to use QKD links to secure the network.

2.3 Objectives of topological optimization for QKD networks

QKD networks and more generally communication networks based on quantum technologies are at their infancy. This especially means that, also link technologies are becoming more and more mature they are currently not deployed over real infrastructures. As a consequence, we don't have any solid input regarding the potential demands and traffic on such networks and as such, are in a very early position to fully specify what could be the objectives of QKD network topological optimization. There are however a number of observation that can be made on the basis of the experience we have so far:

- Links are intrinsically limited in distance, and the attached QKD devices constitute expensive resources. On objective is thus to find the typical distances between QKD devices that minimize the cost of operation of the network
- QKD links are limited in rate, and one objective of building QKD networks is to mutualize the rate of individual links to reach higher throughput through the network than what is possible with one single link.
- Another very important feature is the network resiliency to attacks and failure, a property that is directly linked to the path redundancy in the network. In combination with topologies ensuring enough redundancies, we shall moreover develop protocols able to exploit the path redundancies to recover from failures and to improve the resistance of the network of secrets against attacks.

Chapter 3

Cost of the QKD network

3.1 Toy model: the one-dimensional-2-users QKD chain toy model

3.1.1 Situation of the problem

We consider a generic demand of secret key rate between two parties: Alice (A) and Bob(B), that can be described by the following parameters: Origin: A ; Destination: B ; Distance(A,B) = L ; Target rate: R_T ;

We want to derive the optimum distance between two QKD nodes, A and B in a simplified situation, corresponding to the asymptotic assumptions one can make on a long-distance and high-rate (typical characteristics of a backbone connection):

- The two QKD nodes are "very far away". We will call L their distance, and $L \gg D_{max}$
- The two QKD nodes are exchanging secret bits at a "very high rate". We will call R_T the target rate between A and B, and $R_T \gg R_0$.

Because of the first condition, many intermediate nodes have to be used as key relays to go from A to B, Because of the second condition, many QKD devices have to be deployed in parallel in adjacent nodes to reach a capacity equal to the target rate.

We make the assumption that many possible node location are available and that we want to choose where to deploy QKD devices in order to minimize the price of the global connection from A to B.

3.1.2 Optimum size of the one-dimensional cell

For symmetry reasons, an optimum solutions corresponds to nodes placed regularly between A and B. We will call l the distance between two intermediate nodes. This distance can be seen a the size of one cell on the connection from A to B.

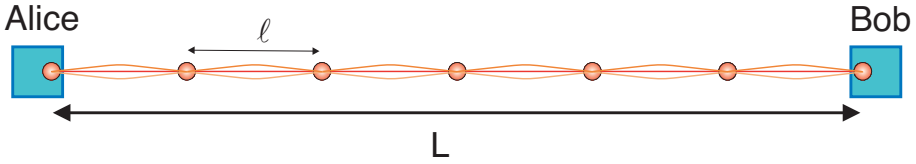

Figure 3.1: The one-dimensional QKD chain: the minimum cost is reached for an optimum value of the cell size l.

There are clearly two effects pushing in different direction regarding the size of the cells:

- on one hand, having large cells allows to minimize the number of intermediate nodes (and since all nodes have to be equipped with QKD devices, this goes in the direction of cost minimization)
- on the other hand, having large cells means that the capacity of a pair of QKD device covering this cell is low, and thus that many QKD devices have to be put in parallel to ensure a given capacity.

The optimum cell size will correspond to the value of l that minimizes the total cost function $\mathcal{C}$

$$\mathcal{C} = C_{QKD}\frac{L}{l}\frac{R_T}{R(l)} = C_{QKD}\frac{L}{l}\frac{R_T}{R_0}e^{l/\lambda_{QKD}} \tag{3.1}$$

We can make several important remarks on this cost function:

- The total cost is directly proportional to the product of the target rate R_T by the total distance L.
- Optimizing the total cost $\mathcal{C}$ is equivalent to minimizing $C(l)/l$ where $C(l) = C_{QKD}/R(l)$ is the per-bit cost of one unit of secret key rate.

It is easy to derive the optimum value of l that minimizes the cost from equation 3.1 by a simple differentiation.

$$\frac{\partial}{\partial l}\mathcal{C} = 0 \Leftrightarrow \frac{d\,(C(l)/l)}{dl} = 0 \Leftrightarrow l = \lambda_{QKD} \tag{3.2}$$

λ_{QKD}, defined in 2.2.5 as a natural scaling parameter for the QKD network appears to be the optimum distance between two consecutive nodes in our simplified model of a long one-dimensional QKD chain. We can observe that this model corresponds to the case where cost is dominated by the cost of QKD devices that have to be deployed. In this case, the total cost is linearly proportional to $R_T \times L$ and the proportionality factor is $C(l)/l$.

Such a cost function is valid only if the contribution of the cost of nodes in the total cost function can be neglected. We will discuss the validity of this assumption in the next subsection.

3.1.3 Taking the cost of nodes into account

Reserving and securing the locations where QKD devices are deployed certainly has a cost. Even though it may be difficult to evaluate, it is very likely that such cost cannot always be neglected with respect to the cost of links. We explicit the expression of the cost function $\mathcal{C}'$ when the cost of nodes is taken into account, which will allow us to discuss the impact of the cost of nodes on the optimum distance between two consecutive nodes on a QKD chain.

$$\mathcal{C}' = C_{QKD}\frac{L}{l}\frac{R_T}{R(l)} + C_n\frac{L}{l} \tag{3.3}$$

The second part of this cost function does not vary depend on the target rate R_T and is purely decreasing with increasing l. Hence the optimum cell size minimizing $\mathcal{C}'$ in equation 3.3 will always be larger than λ_{QKD}, the value minimizing $\mathcal{C}'$ in equation 3.1.

We have plotted on figure 3.2 the variation of the optimum cell size l (in units of λ_{QKD}) with respect to the reduced coordinate of the problem:$C_n/C_{QKD} * R_0/R_T$.

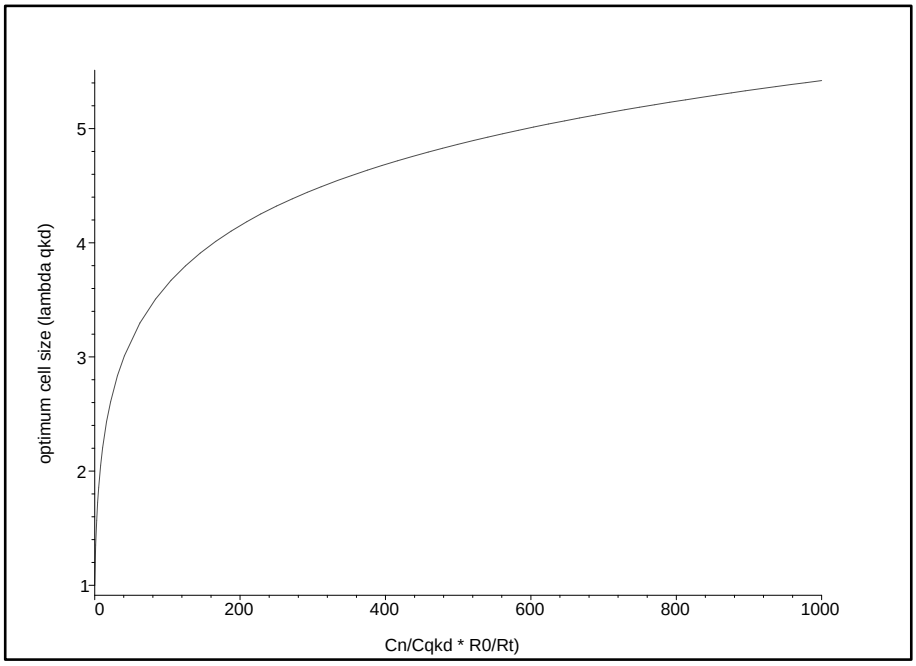

Figure 3.2: Variation of the optimum value of l/λ_{QKD} minimizing equation 3.3 with respect to $C_n/C_{QKD} \times R_0/R_T$.

Figure 3.2 allows us to discuss quantitatively the "weight" of the nodes in the behavior of the cost function.

We can see that the influence of the node cost is potentially important and can lead to an optimum size cell that can be significantly larger than $\lambda_Q KD$ and that could even be in the D_{max} region. In that case, the linear approximation made for $R(l)$ would not be valid and the saturation occuring around D_{max} should be taken into account.

For example, in case the target rate R_T is equal to R_0, we see that the optimum size of QKD links deviates strongly from λ_{QKD} if the cost of one node C_n is more than a 100 times superior to the cost of a pair of QKD devices C_{QKD}.

If $R_T \gg R_0$ the influence of node cost on the total cost function is however much more reduced. We will make this assumption in the next sections relative to the cost optimization of the QKD networks, which will allow us to neglect the cost of QKD nodes.

3.2 Cost of a two-dimensional QKD network: the backbone model

We have studied in section 3.1 the problem of relating the topology of the QKD network with its cost optimization through a simple 1D model and found that provided the cost of QKD nodes can be neglected, the optimum size of QKD links is given by the value of l minimizing $C(l)/l$, where C(l) is the per-bit cost of one unit of secret key rate as a function of the length of the QKD link.

We want to know if such a behavior remains valid when we consider two-dimensional networks and more specifically QKD backbone networks on which we will focus our studies.

3.2.1 What is a QKD 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, what we call the *backbone QKD network* is an infrastructure for key transport that gathers the traffic of secret key between individual pair of users.

Since the SECOQC project is focused on studying network infrastructure for long-distance key distribution, it is necessary to look for network architectures compatible with this goal. A backbone QKD network gathering the traffic emerging from end users is a natural solution. How such infrastructure should look like is what we will try to determine: because QKD links are intrinsically limited in distance, it is not possible to use very long links as it can be for example the case on the Internet. The solution we propose is based on gathering locally the traffic from individual end users to backbone QKD nodes. This mutualized traffic is then routed "hop-by-hop" over the backbone architecture. We can list some requirements on the backbone QKD network:

- It must be resilient to failure and attacks and thus have a high connectivity.
- This architecture must be able to transport an important traffic, therefore we should allow to deploy multiple QKD links (also called QKD trunks) between backbone QKD nodes, as in the one-dimensionnal QKD chain model.

3.2.2 Backbone cells

The corollary to the backbone architecture is that local traffic must be sent to the backbone structure according to some specific rule that will constitute the access network policy.

In the following of this document, the rule we will consider is to associate, to each backbone node, a region of the plane that we will call the backbone cell and that all users located within a given backbone cell send their traffic, via an direct access QKD link to the backbone node.

A natural way to model the backbone network will be through stochastic modeling [12]: in this context, if $\{N_i\}$ is the set of backbone nodes, distributed over the plane, the corresponding backbone cells are the convex polygones $\{\mathcal{V}_i\}$ known as the Voronoï cells with nucleus $\{N_i\}$. Each Voronoï cell $\mathcal{V}_i$ is constructed by taking the intersection of the half-planes bounded by the bisectors of the segment $[N_i, N_j]$ and containing N_i. The systems of all the cells creates a tessellation of the plane called the Voronoi tesselation (see figure 3.3).

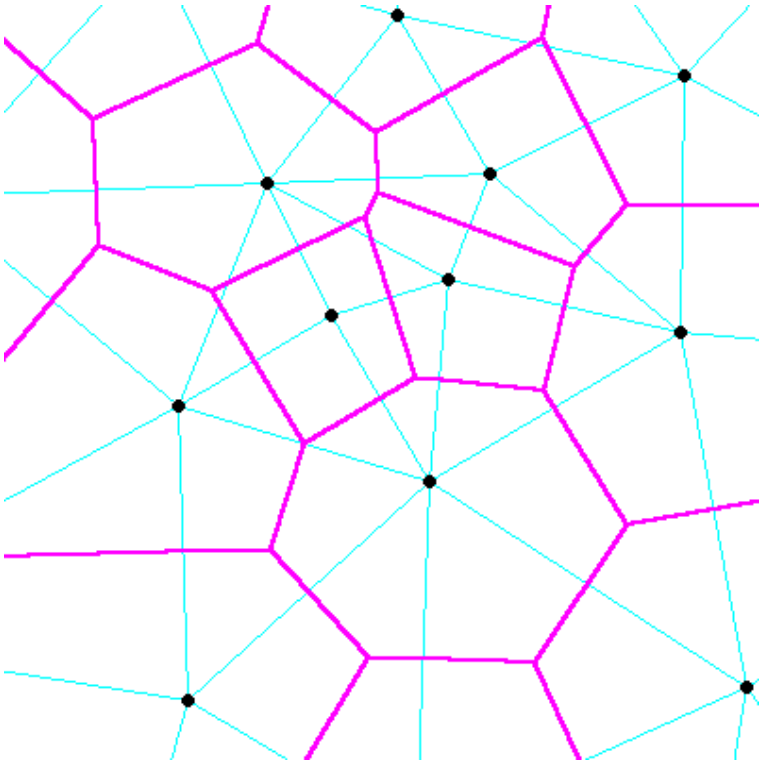

Figure 3.3: In purple: Voronoi tesselation associated to a distribution of points. In blue: the Delaunay graph, connecting the center of neighbor Voronoi cells. In the backbone QKD network, backbone QKD links will indeed correspond to the Delaunay graph associated to the distribution of backbone nodes.

3.2.3 Routing traffic in the QKD network

The existence of a backbone is synonymous with the existence of a *hierarchy* within the QKD network. Indeed there we will be at least one level of hierarchy in the way communications are routed over the network in our backbone model. For a given origin-destination pair of users (A,B), the traffic R_{AB} is routed in the following way:

- The traffic goes from A to its nearest QKD backbone node N_A (center of the backbone cell containing A), through a single QKD link, that we will call an access link.
- The traffic is routed through the shortest over the backbone QKD network from N_A to N_B (QKD node closer to B).
- The traffic goes from N_B to B.

More hierarchical levels within the backbone network could be considered. We will however not consider this problem within this document and leave aside for further studies.

3.2.4 Geometrical models of backbone

Determining the length of the shortest path in a given backbone network of arbitrary topology may not be a tractable problem. Since we are interested in studying models for which analytical formulas can be derived, we have considered two types of geometry for the backbone network:

1. A square backbone QKD network (see section 3.5, 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 N_A, N_B can be designated by cartesian coordinates (x_A, y_A), (x_B, y_B) and the shortest path length is simply $|x_A - x_B| + |y_A - y_B|$.
2. A Voronoï backbone network, on which we can define a routing technique for which the distribution of length can be determined.

3.2.5 Modeling traffic demand and user distribution

We are interested in deriving cost functions for the QKD backbone network and use this information to characterize how backbone QKD networks should be dimensioned. However cost function cannot be derived without extra assumptions on the traffic supported by the network. A backbone infrastructure is typically needed to support the communication needs of *many* users, knowing that each pair of user can generate a communication. As we have seen from the toy model, the cost of accommodating one demand is a function of two factors:

1. The traffic demand, i.e the rate of secret key between two users. Since we are working with a flow model, rates are expressed by a single value, that can be seen as an average of the dynamical rate over time.
2. The distance between the origin and the destination of a demand: for a given demand, the larger the distance, the higher the cost.

In the case of the backbone network, the complete characterization of traffic and user distribution would require a very large number of parameters. We however do not need to go in such a level of detail in our generic model [1] and we will make simplifying assumptions on traffic demand and user distribution in order to derive a cost function.

Assumption on traffic demand

Since we have no a priori model for the traffic demand, we will basically let that point aside in this document and make the following assumption:
The amount of communication is supposed to be identical between each possible pair of users. In particular it is independent of their distance).

User distribution and spatial extension of the network

The problem that may arise from the assumption on traffic is that the rates supported by the backbone network may not be finite, even with a finite number of users.

To cope with this effect, we have decided to study the cost function of the backbone QKD network over a large but bounded region of the plane. This assumption consists in considering that users of the QKD network are located on a bounded region of extension $D \sim L \times L$.

[1] It is also true that we do not have the complete information combining user distribution with traffic demand. Such information typically depends on the usage / application run on a network and we so far have little insight on the profile of communications that will be exchanged over QKD networks.

Unlike the rather drastic assumption made on traffic demands that are supposed to be totally uniform, we will not automatically make extra simplifying assumptions on the user distribution.

3.3 General form of the cost function of the QKD backbone network derived with stochastic modeling

Stochastic geometry is a very useful mathematical tool to model telecommunication networks. It has the advantage of being able to catch the essential spatial characteristics of a network through a small number of parameters [12]. It thus allows to abstract some general characteristics of a given network, like the behavior of its cost function, under a restricted set of assumptions. This approach fits very well with the objectives of this document, and we put some effort in modeling a QKD backbone network with stochastic tools.

In the calculations on a regular square backbone network the user distribution will be modeled by a Poisson stochastic point process, characterized by its intensity density f, defined over the support $D \sim L \times L$.

We denote by $\Pi = \sum_i \delta_{U_i}$ the Point process for the users, and assume that Π is a Poisson point process with intensity density $f(x)$ satisfying $\mu := \int f < \infty$.

Let $N = \sum_i \delta_{X_i, D_i}$ denote the point process of backbone nodes and cells of the QKD network. We assume that $\cup_i D_i$ covers the support of f and that for all i, f integrates to zero on the domain $D_i \cap (\cup_{j \neq i} D_j)$.

The set of assumption made in 3.2.5 allow us to make a general derivation of the per-bit cost of a secret key exchange over the network for one communication and then to average it over the whole network:

Per-bit cost for one communicaton

The per bit cost of a communication between user u and v, under the routing scheme described previously can be summarized under the following formulas:

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

where $C = C(l)$ is the per bit cost over a single QKD link and C^{hop} is a per bit cost of one hop on the backbone network represented by the point process N, between the nodes X_i and X_j. C^{hop} is calculated under the same hypothesis used in 3.1 and we simply have $C^{\text{hop}}(i, j; N) = C(|X_i - X_j|)$.

Mean Per-bit cost of secret key exchange over the QKD network

Since QKD links are undirected, communication cost should not be counted twice in the total cost and the mean per byte cost summed over all possible pairs of communications is

then

$$\begin{aligned}
\frac{1}{2}\mathbb{E}[\sum_{k\neq l}\mathcal{C}(U_k,U_l;M)] &= \frac{1}{2}\int \mathcal{C}(u,v;M)\,f(u)\,f(v)\,du\,dv \\
&= \frac{1}{2}\sum_k \int_{D_k\times D_k} \{C(u-X_k)+C(v-X_k)\}\;f(u)\,f(v)\,du\,dv \\
&\quad + \frac{1}{2}\sum_{k\neq l}\int_{D_k\times D_l} \left\{C(u-X_k)+C(v-X_l)+C^{\text{hop}}(k,l;M)\right\}\;f(u)\,f(v)\,du\,dv \\
&= \frac{1}{2}\sum_k\sum_l \int_{D_k\times D_l} \{C(u-X_k)+C(v-X_l)\}\;f(u)\,f(v)\,du\,dv \\
&\quad + \frac{1}{2}\sum_{k\neq l}\int_{D_k\times D_l} C^{\text{hop}}(k,l;M)\,f(u)\,f(v)\,du\,dv \\
&=: C^{\text{loc}} + C^{\text{bb}}\ .
\end{aligned}$$

As we can see, the per-bit cost of communication over the QKD network can be split in two contributions:

1. The local cost, C^{loc} can be associated with the cost of connecting users to the backbone network. It is thus the cost of the QKD access network.
2. The backbone cost C^{bb}, i.e the portion of the per-bit cost that is supported by the backbone part of the network.

3.4 Cost of the local access network

Reduced notations

We can define

$$\begin{aligned}
\mu_k &:= \int_{D_k} f(u)\,du\ ; \\
\gamma_k &:= \int_{D_k} C(|u-X_k|)\,f(u)\,du\ ;
\end{aligned}$$

respectively the mean number of users and the cost of access links in cell D_k.
The local cost is thus the product of the mean total number of user by a parameter γ characterizing solely the access network:

$$C^{\text{loc}} = \left(\sum_k \mu_k\right)\left(\sum_l \gamma_l\right) = \mu\,\gamma\ , \tag{3.4}$$

where

$$\gamma := \int C^{(loc)}(u)\,f(u)\,du\ ,$$

and $C^{(loc)}(u)$ is the per bit cost of the local connection to the network from point u,

$$C^{(loc)}(u) := \sum_k C(|u-X_k|)\,\mathbf{1}_{D_k}(u)\ .$$

Approximation for f smooth

By f smooth, we mean that it stays approximately constant on every cell D_k, i.e., for all k and $u \in D_k$, we have

$$f(u) \simeq \frac{\mu_k}{\mathrm{Leb}(D_k)} ,$$

where $\mathrm{Leb}(D_k)$ the Lebesgue measure of D_k (in the appropriate dimension). In this equation, $\simeq$ can be replaced by an equality if f is constant over D_k. It follows that

$$\gamma \simeq \sum_k \mu_k \frac{1}{\mathrm{Leb}(D_k)} \int_{D_k} C(|u - X_k|)\, du .$$

If N is translation invariant, then

$$\overline{C} := \frac{1}{\mathrm{Leb}(D_k)} \int_{D_k} C(|u - X_k|)\, du$$

or, in a random stationary and independent from N setting for M, we may take the mean

$$\overline{C} := \mathbb{E}\left[\frac{1}{\mathrm{Leb}(D_k)} \int_{D_k} C(|u - X_k|)\, du \right] ;$$

in both cases, $\overline{C}$ does not depend on k and we finally obtain

$$C^{\mathrm{loc}} \simeq \mu^2\, \overline{C} .$$

3.5 Cost of the square backbone QKD network

Network model

For simplicity reasons, we have considered, as a first example, the case of a QKD backbone network that has a perfectly regular topology and for which it is simple to compute the shortest path length between two backbone nodes.

The architecture we consider is the following: users are distributed over a large area of size L by L and the backbone QKD network is a regular graph of degree 4, i.e 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 on figure 3.4. The free parameter on which we will perform the cost optimization is the size of backbone cells l. We will moreover make the assumption that the user density function, f is uniform over D.

Computation of C^{bb} for the square network

Here we set $X_k = k\ell$ and $D_k = X_k + \ell[-1/2, 1/2]^2$ with $k \in \mathbb{Z}^2$ and, for all $k \neq l$,

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

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

Using the notation introduced in 3.4 we have:

$$C^{\mathrm{bb}} = \frac{1}{2} \sum_{k \neq l} \mu_k \mu_l\, C^{\mathrm{hop}}(k, l; M) , \tag{3.5}$$

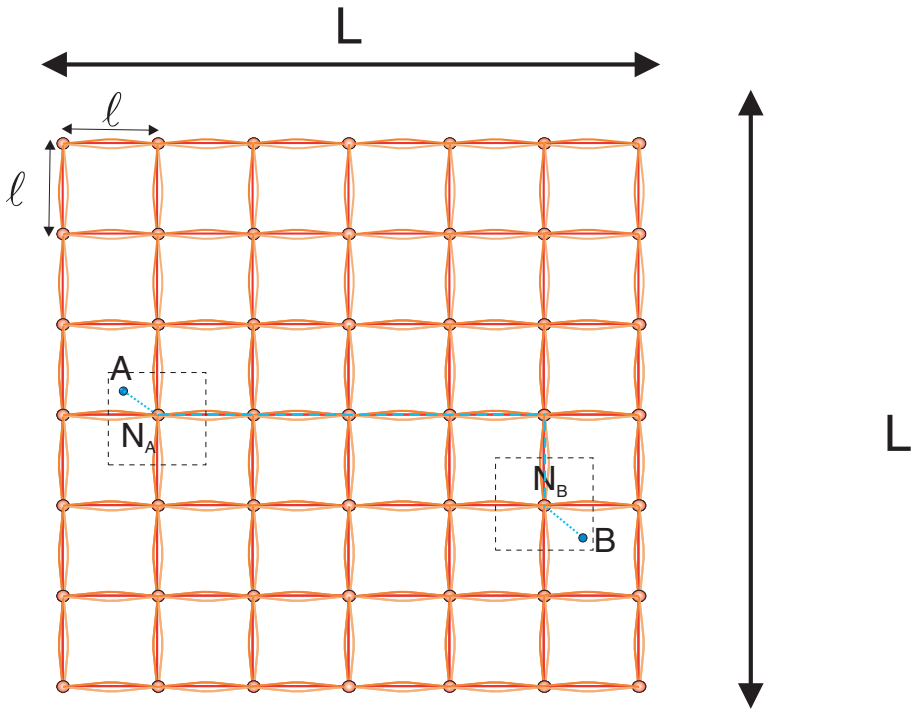

Figure 3.4: Structure of a two-dimensional regular square backbone network: a regular array of cells of dimension l paves a region of size L by L. User distribution is described by a random point process. In each cell, a central node collects all the local traffic. Every user in the cell is thus connected 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 trough on a shortest path basis. The dotted blue line describes the path followed by a communication between two users A and B (see text for more details).

Hence, by (3.5), we obtain

$$C^{\text{bb}} = \frac{1}{2}\, C(\ell)\, \boldsymbol{\mu}^T \Gamma \boldsymbol{\mu}\ ,$$

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 $\Gamma_{k,l} = \|k-l\|_1$.

As mentioned in the description of the network model we suppose that the density intensity $f(u)$ is constant on its support D, where $D := \bigcup_{k\in\{0,\ldots,N-1\}^d} D_k$. Since μ stands for the mean number of users over D, the user density is μ/L^2 and we have $f(u) = \mu/\,L^2\,\mathbf{1}_D(u)$. The mean number of users in cell k, μ_k is constant for all cells D_k: $\mu_k = \mu/N^2$.

In this case, we find

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

Now, we compute

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

where the asymptotic equivalence holds as $N\to\infty$. Hence for any ℓ, we obtain, as $N\to\infty$,

$$C^{\text{bb}} \sim \frac{1}{2}\,\frac{\mu^2}{N^4}C(\ell)\,\frac{2}{3}\,N^5 = \frac{2}{3}\,\frac{C(\ell)}{\ell}\,\frac{\mu^2}{2}\,L\,.$$

In the latter expression, we have four multiplicative terms

1. $2/3$, a constant only depending on the dimension and the geometry of the backbone network (for a cube in dimension d, we could generalize our calculation and would find $d/3$) ;
2. $C(\ell)/\ell$, a cost function only depending on the distance ℓ between the stations of the backbone;
3. $\mu^2/2$, the square of the mean number of user, i.e with our communication model, the mean number 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.

It is interesting to consider this result on C^{bb} in comparison with the result we have on C^{loc} from 3.4: $C^{\text{loc}} \simeq \mu^2\,\overline{C}$ where $\overline{C}$ stands the per-bit cost function C averaged over one cell. In the case of the square network of size l a square local cell is contained between two circles of radius $l/2$ and $l\,\sqrt{2}/2 < l$. Since C is an increasing function of distance we have anyway always have $\overline{C} < C(l)$, and we can thus draw the following result:

In the limit of large networks, i.e for $L \gg l$ the backbone cost is dominant over the local cost. Since it scales like $C(l)/l$ with the backbone cell size l, the optimum size cell for large QKD networks in our model is $l_{opt} = \lambda_{QKD}$.

Conclusion

In this document we have presented the first results of some recent work initiated within the Secoqc project, aiming at understanding the typical behavior of QKD network cost functions through simple models for which analytical calculations are tractable.

We believe that the important first conclusions that can be drawn from the obtained results is that the optimum distance of QKD links operated within full QKD networks departs from the common trend in the field where almost all the attention has been put on the maximum distance of a single link.

Combining links to form a network naturally leads to a the problem of the optimum working point of QKD links. Due to the specific cost versus distance typical behavior of QKD links, with an exponential decrease of rate with distance, it appears that cost optimization will tend to push QKD network developers to operate the links under distances where the secret key rates remains high, i.e for moderate amount of losses.

Bibliography

[1] L. Salvail, D-SEC-17, *Rough Network Architecture for Quantum Communication*, Secoqc Deliverable.

[2] R. Alléaume, K. Kraus and O. Maurhart , Technical Report *TR-NET-01 Secoqc QKD network*, sept 2005.

[3] R. Alléaume, K. Kraus and O. Maurhart , Technical Report *TR-NET-01 Secoqc QKD network*, sept 2005.

[4] R. Alléaume, T. Länger, T. Lorünser, A. Marhold, O. Maurhart, M. Peev, *Work plan of the SECOQC Subproject ÒSystem ImplementationÓ (SI)* December 2005.

[5] J. Dégila and B. Sansò, A survey of topologies and performance measures for large-scale networks, IEEE Communications Surveys & Tutorials, fourth quarter 2004.

[6] P. Gupta and P. R. Kumar, *The Capacity of Wireless Networks*, IEEE Transactions of information theory, VOL. 46, NO. 2, March 2000.

[7] H. Tangmunarunkit, R. Govindan, S. Jamin, S. Shenker, W. Willinger, *Network topology generators: degree-based vs structural*, Proceedings of the ACM SIGCOMM, August, 2002.

[8] E. Zegura, K. L. Calvert and M. J. Donahoo, *A quantitative comparison of graph-based models for Internet topology*, IEEE Transactions on networking, VOL. 5, NO.6, December 1997.

[9] S. H. Strogatz, Exploring complex networks, Nature, VOL. 410, pp268-276, March 2001.

[10] R. Albert, J. Hawoong, A.-L. Barabási, *Error and attack tolerance of complex networks*, Nature, VOL. 406, pp378-382, July 2000.

[11] P. Crucitti, V. Latora, M. Marchiori and A. Rapisarda, *Efficiency of Scale-Free Networks: Error and attack tolerance*, arxiv:cond-mat/0205601.

[12] F. Baccelli, M. Klein, M. Lebourges, S. Zuyev, *Stochastic geometry and architecture of communication networks*, Telecommunications Systems 7, pp 209-207, 1997.

[13] H. Bechmann-Pasquinucci, N. Cerf, M. Dusek, N. Lütkenhaus, V. Scarani, M. Peev, *Report on a QIT-perspective comparison of the different platforms with respect to the evaluation criteria set in phase I of SECOQC* sept 2005.

[14] H.Zbinden, H.Bechmann-Pasquinucci, N.Gisin, G.Ribordy, Appl. Phys. B67 (1998)743-748.

[15] H Kosaka, A Tomita, Y Nambu, T Kimura, K Nakamura, Single-photon interference experiment over 100 km for quantum cryptography system using a balanced gated-mode photon detector IEEE Electronics letter 2003.