Self-Adaption of Quantum Key Distribution Devices to Changing Working Conditions

Sandra König
Safety & Security Department
Austrian Institute of Technology, Klagenfurt, Austria
Sandra.Koenig@ait.ac.at

Stefan Rass
Department of Applied Informatics, System Security Group
Universität Klagenfurt, Universitätsstrasse 65-67
9020 Klagenfurt, Austria
stefan.rass@uni-klu.ac.at

***Abstract*—Quantum key distribution (QKD) draws security from the ability to detect eavesdroppers upon the incident of "unnaturally high" quantum bit error rates (QBER) during the protocol. This presumes that a working QKD device implementation needs to be calibrated with its own individual and characteristic channel noise that is observed in any case, especially when there is no eavesdropper. This natural noise level influences the idle QBER, and is in turn dependent on the device's working conditions. This work describes a statistical approach to construct a model that can be used to continuously compute the normal QBER, based on current (and changing) working conditions. The model is thus meant as a tool to refine the theoretical QBER threshold specific to the given QKD protocol, based on empirical data obtained under the given environmental conditions. More importantly, it allows the QKD-device to self-recalibrate under changing working conditions.**

***Keywords*–copula; estimation; quantum network; quantum devices; statistics**

I. Introduction

The unique feature of quantum key distribution (QKD) is its ability to detect passive eavesdropping. This remarkable ability rests on a fundamental result of quantum physics that rules out the possibility of creating a perfect copy of a single photon [1]. Consequently, passive eavesdropping attempts will unavoidably introduce errors on a quantum channel that would otherwise deliver quantum bits (qubits, photons) under some specific and characteristic channel noise and error frequency.

Recent experimental findings on the quantum key distribution network demonstrated as the result of the EU project SECOQC (summarized in [2]) raised the question of how much environmental influences affect the "natural" quantum bit (qubit) error rate (QBER) observed on a quantum line that is not under eavesdropping attacks. A measurement sample reported in [3] was used to gain first insights in the problem, but the deeper mechanisms of dependency between QBER and the device's working conditions have not been modeled comprehensively up to now.

The desire of having a model that explains how the QBER depends on environmental parameters like temperature, humidity, radiation, etc. is motivated by the problem of finding a good calibration of QKD devices, so that the channel performance is maximized. Unfortunately, with the QBER being known to depend on non-cryptographic parameters, it is difficult to give reasonable threshold figures that distinguish the natural error level from that induced by a passive eavesdropping. We spare the technical details on how a QBER threshold is determined for a given QKD protocol here (that procedure is specific for each known QKD protocol and implementation), and focus our attention on a statistical approach to obtain a model of interplay between the qubit error rate and various environmental parameters.

To this end, we utilize a general tool of probability theory, a *copula function*, to separate the parameter model (probability distribution of a single environment parameter) from the interdependency model (which is the copula function). In that regard, we use Section II to refresh the reader's memory on copula theory to the extent required here to get to the point where we can give effective methods to infer an expected qubit error rate upon known external influence parameters.

More precisely, our work addresses the following problem: *given the current working conditions of a QKD device, what would the natural qubit error rate be, whose transgression would indicate the presence of an eavesdropper?* The basic intention behind this research is aiding practical implementations of QKD-enhanced networks, where our models provide a statistically grounded help to react on changing environmental conditions. The remainder of this work is structured as follows: after theoretical groundwork in Section II, we move on by showing how to use empirical data (measurements) drawn from a given device to construct an interdependency model that explains how the QBER and other variables mutually depend on one another. Section IV then describes how to single out the QBER from this overall dependency structure towards computing the expected error rate from the remaining variables. The concluding Section V summarizes the procedure and provides final remarks.

Related Work

Surprisingly, there seem to be only few publications paying attention to statistical dependencies of cryptographic parameters and the working conditions of a real device, such as [3], [4]. While most experimental implementations of QKD, such as [2], [5]–[8] give quite a number of details on device parameters, optimizations of these are mostly out of focus. An interesting direction of research is towards becoming "device-independent" [9], [10], which to some extent may relieve issues of hacking detection facilities, yet leaves the problem of optimal device configuration nevertheless open. The idea of self-adaptation is not new and has already seen applications in the quantum world [11]–[13] including the concept of copulas, applications of the latter to the end of self-adaption remain a seemingly new field of research. Copulas have been successfully applied to various problems of explaining and exploiting dependencies among various risk factors (related to general system security [14], [15]), and the goal of this work is taking first steps in a study of their applicability in the yet unexplored area of self-configuring quantum devices.

 ISBN: 978-1-61208-380-3

II. Preliminaries and Notation

We denote random variables by uppercase Latin letters $(X, Z, \ldots)$, and let matrices be uppercase Greek or bold-printed Latin letters $(\Sigma, \mathbf{D}, \ldots)$. The symbol $X \sim F(x)$ denotes the fact that the random variable X has the distribution function F. For each such distribution, we let the corresponding lower-case letter denote its density function, i.e., f in the example case.

For self-containment of our presentation, we give a short overview of the most essential facts about copulas that we are going to use, as for a more detailed introduction we refer to [16].

Definition II.1. *A* copula *is a (n-dimensional) distribution function* $C : [0,1]^n \to [0,1]$ *with uniform marginal distributions.*

Especially, a copula satisfies the following properties:

Lemma II.1.
1) *For every* $u_1, \ldots, u_n \in [0,1]$, $C(u_1, \ldots, u_n) = 0$ *if at least one of the arguments is zero and*
2) $C(u_1, \ldots, u_n) = u_i$ *if* $u_j = 1$ *for all* $j \neq i$.

A family of copulas that leads to handy models in higher dimensions is known as the family of Archimedean copulas, of which many extensions exist.

Definition II.2. *An* Archimedean copula *is determined by the so called* generator function $\phi(x)$ *via*

$$C(u_1, \ldots, u_n) = \phi^{-1}(\phi(u_1) + \ldots + \phi(u_n)). \qquad (1)$$

The generator function $\phi : [0,1] \to [0,\infty]$ *has to satisfy* $\phi(1) = 0$ *and* $\phi(\infty) = 0$*, furthermore,* ϕ *has to be* n-monotone*, i.e., to be differentiable up to order* $n-2$ *with* $(-1)^{n-2}\phi^{(n-2)}(t)$ *being nondecreasing and convex and*

$$(-1)^i \phi^{(i)}(t) \geq 0 \text{ for } 0 \leq i \leq n-2$$

for all $t \in [0, \infty)$.

As one of the cornerstones in copula theory, *Sklårs theorem* connects these functions to the relationship between n univariate distribution functions and their joint (multivariate) distribution:

Proposition II.2. *Let the random variables* $X_1, \ldots, X_n$ *have distribution functions* $F_1, \ldots, F_n$ *respectively and let* H *be their joint distribution function. Then there exists a copula* C *such that*

$$H(x_1, \ldots, x_n) = C(F_1(x_1), \ldots, F_n(x_n))$$

for all $x_i, \ldots, x_n \in \mathbb{R}$.
If all the F_i*s are continuous, then the copula* C *is unique.*

The usefulness of this result lies in the fact that the joint distribution function of $X_1, \ldots, X_n$ can be decomposed into n univariate functions $F_1, \ldots, F_n$ that describe the behaviour of the individual variables and another component (namely the function C) that describes the dependence structure, which allows to model them independently.

Turning things around it is also possible to extract the dependence structure from the marginal distributions F_i and the joint distribution H via

$$C(u_1, \ldots, u_n) = H(F_1^{-1}(u_1), \ldots, F_n^{-1}(u_n)) \qquad (2)$$

where $F_i^{-1}(u)$ denotes the pseudo-inverse of $F_i(x)$, which is given by $F_i^{-1}(u) = \sup\{x | F_i(x) \leq u\}$. A special case of this connection between Copula and random variables leads an alternative characterization of independence, which is usually written as $H(x_1, \ldots, x_n) = F_1(x_1) \cdot \ldots \cdot F_n(x_n)$.

Example II.3. *If the (unique) copula from (2) turns out to be the product copula* $C(u_1, \ldots, u_n) = u_1 \cdot \ldots \cdot u_n$*, then the random variables* $X_1, \ldots, X_n$ *are independent.*

III. A Copula Model of the QKD network

A. Summary of the Data

A summary of the results obtained from an implemented QKD network in Vienna [2] can be found in [4]. The following quantities were measured and are used here (abbreviation in brackets): qubit error rate in percentage terms (QBER), air temperature (TEMP), relative humidity (HUM), sunshine duration in seconds (DUR), global radiation in watt/m^2(RAD).

Since we are here focusing on the relationship between QBER and environmental quantities, we only use data that were measured on the same device to avoid getting biased results. The quantiles of our sample of size $n = 276$ are displayed in Table I.

TABLE I. Quantiles of measured quantities

	min	$q_{0.25}$	median	$q_{0.75}$	max
QBER	98.00	132.75	147.00	163.00	212.00
TEMP	117.00	134.75	148.00	163.00	184.00
HUM	71.00	80.00	84.00	91.00	93.00
DUR	0.00	0.00	0.00	0.00	600.00
RAD	0.00	0.00	0.00	146.00	539.00

Throughout the rest of the paper, let $\mathbf{D}$ denote the data matrix that comprises the entirety of samples as a table whose headings correspond to the row labels in Table I. Thus, the matrix $\mathbf{D}$ is of shape $(n \times 5)$ for our $n = 276$ samples, and has entries $(X_1, \ldots, X_5)$ modeling the measurements of (QBER, TEMP, HUM, DUR, RAD) as random variables.

B. Building up a Model

Mainly interested in the dependence structure, we do not make explicit assumptions about the distributions of each quantity but rather use their empirical distribution to transform them into pseudo-observations $U_1, \ldots, U_n$ that are uniform $(0,1)$-distributed. A basic first choice is to consider a multidimensional copula C that models the joint distribution H of all the quantities via $H(x_1, \ldots, x_n) = C(U_1, \ldots, U_n)$. Fitting a copula is usually done by maximizing the log-likelihood function

$$\ell(x_1, \ldots, x_n) = \log\left[c\left(u_1, \ldots, u_n\right)\right],$$

with c denoting the density of the copula C. In a general setting, this can easily become infeasible in our five-dimensional case, so we first choose a parametric family C_θ of copulas and then seek the parameter θ that maximizes the one-dimensional function

$$\ell(\theta) = \log\left[c_\theta\left(u_1, \ldots, u_n\right)\right].$$

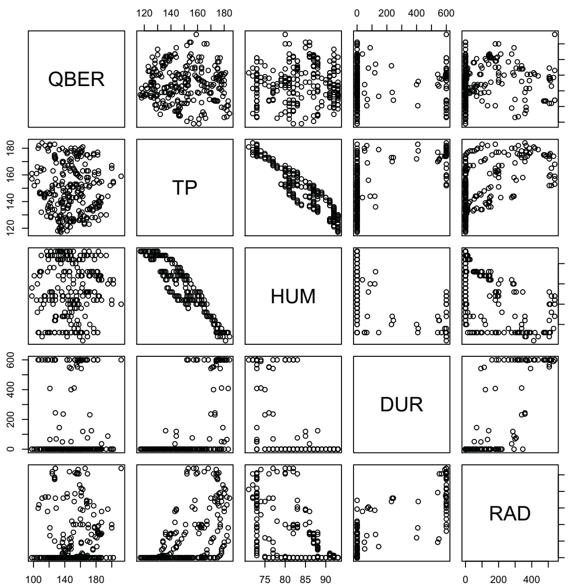

Figure 1. Pairwise correlations among variables

As for the parametric family, we first choose the *Gumbel copula*, which is generated by $\phi(t) = (-\ln(t))^\theta$, yielding

$$C(u_1, \ldots, u_n) = \exp\left\{-[(-\ln(u_1))^\theta + \ldots + (-\ln(u_n))^\theta]^{1/\theta}\right\}.$$

A p-value of zero clearly shows that this model is not describing the data properly.

The above model is simple to construct and to use but it also has its weaknesses: firstly it describes the behaviour of five random variables with just one number and secondly its components are all exchangeable. Taking a closer look at the pairwise correlations of the considered quantities (see Figure 1) shows that this exchangeability is not fulfilled in our case.

To take care of possibly different correlations among the occurring variables, we consider a more flexible model called *nested* copulas (sometimes also called hierarchical copulas) which is often used in finance, see for example [14]. The basic idea of a nested copula model is to use several copulas at different levels to describe the relation between the variables.

For clarity of such a hierarchically constructed probability distribution, we use a graphical tree-notation like shown in Figure 2 to "depict" the (otherwise complicated) distribution function. To formally specify the latter, we introduce some notational conventions: at each level $\ell \in 1, \ldots, L$ (counting bottom-up in the hierarchy tree) we have n_ℓ copulas, where $C_{\ell,j}$, $j \in 1, \ldots, n_\ell$, is the $j-$th copula at level ℓ. Further, every copula $C_{\ell,j}$ has dimension $d_{\ell,j}$ that gives the number of arguments u_i that directly or indirectly enter this copula.

Two special cases are shown in Figure 2 for the four-dimensional case: the fully nested copula which adds one dimension at each step (left side) and a partially nested copula where the number of copula decreases at each level (right side). Formally, a fully nested copula is defined by

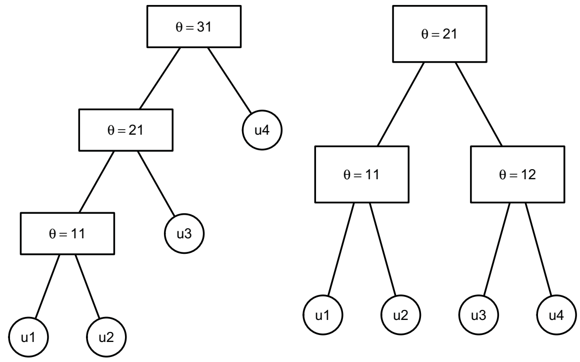

Figure 2. Fully nested vs. partially nested copula

$$\begin{aligned} &C(u_1, \ldots, u_n) = \\ &\phi_{n-1}^{-1}[\phi_{n-1}(\ldots[\phi_2(\phi_1^{-1}[\phi_1(u_1) + \phi_1(u_2)] + \phi_2(u_3)] \\ &+ \ldots + \phi_{n-2}(u_{n-1})) + \phi_{n-1}(u_n))], \end{aligned} \tag{3}$$

where the occurring generator functions $\phi_1, \ldots, \phi_{n-1}$ may come from different families of Archimedean copulas.

All in all, the dependence structure is determined by $n-1$ parameters (instead of just one as in the model above) and there are $\frac{n(n-1)}{2}$ different bivariate margins.

The partially nested copula may be defined similarly, for reasons of clarity and comprehensibility we here give the expression for $n = 4$, corresponding to the case shown in the right side of Figure 2:

$$\begin{aligned} C(u_1, u_2, u_3, u_4) =& \phi_{21}^{-1}[\phi_{21}(\phi_{11}^{-1}[\phi_{11}(u_1) + \phi_{11}(u_2)] \\ &+ \phi_{21}(\phi_{12}^{-1}[\phi_{12}(u_3) + \phi_{12}(u_4)])], \end{aligned} \tag{4}$$

where the generator ϕ_{ij} is from the jth copula on the ith level, usually denoted by C_{ij}.

Finding a suitable nested copula model may quickly become laborious since one might have to check all possible subsets of variables and compare the goodness of fit of the corresponding estimated copula. Handling this problem in `R`, one may use the package `HAC`, introduced in [17]. In our case, we find that a suitable model consists of four two-dimensional Gumbel copulas, which are defined as follows:

Definition III.1. *A* Gumbel copula *is an Archimedean copula that is generated by*

$$\phi(t) = (-\ln(t))^\theta$$

for $\theta \geq 1$.
In the two-dimensional case, the copula is explicitly given by

$$C(u, v) = \exp\left[-\left((-\ln(u))^\theta + (-\ln(v))^\theta\right)^{\frac{1}{\theta}}\right] \tag{5}$$

for $u, v \in [0, 1]$.

The dependence structure between the considered quantities is shown in Figure 3.

It is known that in a nested copula model with a Gumbel generator the parameters have to decrease with the level (see [14] for fully nested copulas and [18] for the general case).

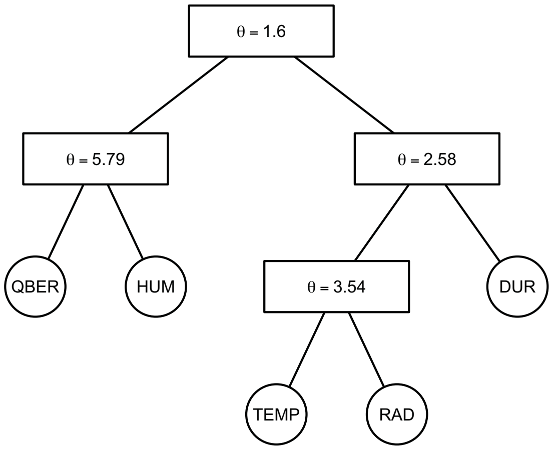

Figure 3. Dependence structure for HAC model

Since in our case the parameters on the upper levels are rather close, we consider a modification of this model by allowing to aggregate Copulas whose parameters do not differ too much. A justification for this approach is the close relation between the parameter θ of the generator and Kendall's tau τ, which is connected to copulas via

$$\tau = 4 \int_{[0,1]^2} C(u,v) dC(u,v) - 1. \tag{6}$$

For Archimedean copulas with generator function $\phi(t)$, it was shown in [16] that (6) simplifies to

$$\tau = 1 + 4 \int_0^1 \frac{\phi(t)}{\phi'(t)} dt, \tag{7}$$

which for the Gumbel copula leads to

$$\begin{aligned} \tau &= 1 - 4 \int_0^1 \frac{(-\log(t))^\theta \cdot t}{\theta(-\log(t))^{\theta-1}} dt \\ &= 1 - \frac{1}{\theta}. \end{aligned}$$

Hence if the parameters of two subsequent copulas are close, so is their dependence when characterized through Kendall's τ and it might be beneficial to model the affected variables with only one copula.

In order to get an impression on how suitable each of the above models is, we adapted the bootstrapping goodness of fit test [19] that was used in the case of a one-parametric copula to the estimation of nested copulas.

In our first 200 trial tests, each of which with a sample size of $N = 1000$ and a confidence level of 0.95, we never got a positive p-value if the tolerance is set to zero. When copulas are allowed to be aggregated, a p-value of 0.014 was found once, which still leads to rejection of the null hypothesis that the data at hand are drawn from a distribution given through this copula. This indicates that some preconditioning of the data matrix might be necessary to get a good fit. One solution for such a preprocessing is described in the next Section.

C. Preconditioning Towards Better Fits

As indicated by our quantum network data, it may occasionally be the case that none of the tried copula-models models the data satisfactorily. More precisely, existing software packages for copula fitting (such as `HAC` in `R`) assume *positive correlations* between all variables of interest. Unfortunately, our experimental QKD prototype supplied data exhibiting *negative* correlations amongst some of the observed variables.

In order to fix this, we can apply a linear transformation $\mathbf{M}$ to the data matrix $\mathbf{D}$ in order to make all pairwise correlations in the transformed data matrix $\mathbf{M} \cdot \mathbf{D}$ strictly positive. To this end, consider the Cholesky-decomposition of the covariance matrix Σ of the data $\mathbf{D}$, given as $\Sigma = \mathbf{L}^T \cdot \mathbf{L} = \mathbf{L}^T \cdot \mathbf{I} \cdot \mathbf{L}$. By the linearity properties of covariance, it is easy to check that the covariance matrix of $\mathbf{D} \cdot \mathbf{L}^{-1}$ is the identity matrix, having zero-correlations among all pairwise distinct variables. It is then a simple matter of multiplication with another invertible matrix (with low condition number to avoid numerical round-off-errors in the inverse transform) with all strictly positive entries to artificially introduce positive correlations, as required in the copula fitting process. Given such a matrix $\mathbf{A}$, the final linear transformation takes the form $\mathbf{D}' := \mathbf{D} \cdot (\mathbf{L}^{-1} \cdot \mathbf{A})$, thus our pre-conditioning transformation matrix is $\mathbf{M} := \mathbf{L}^{-1} \cdot \mathbf{A}$, where $\mathbf{L}$ comes out of the Cholesky decomposition of the original covariance matrix Σ, and $\mathbf{A}$ can be chosen freely, subject to only positive entries and good condition number (for numerically stable invertibility).

In our experiments, we used a bootstrap fitting with tolerance $\varepsilon = 0.4$. We constructed $\mathbf{A}$ as a 5×5-matrix having Gamma-distributed entries (with shape-parameter 5 and scale-parameter $1/2$). In 5 out of 200 trials, the p-value after preconditioning with $\mathbf{M} = \mathbf{L}^{-1}\mathbf{A}$ was larger than 0.05. The best fit giving $p = 0.613$ was obtained under the transformation coefficients (rounded to three decimals after the comma)

$$\mathbf{M} = \begin{pmatrix} 0.122 & 4.444 & 0.378 & 1.634 & 4.384 \\ 0.650 & 0.870 & 1.321 & 0.941 & 2.293 \\ 0.606 & 3.326 & 0.763 & 2.172 & 2.102 \\ 2.534 & 0.415 & 2.055 & 1.969 & 1.659 \\ 2.668 & 2.031 & 3.590 & 2.241 & 1.015 \end{pmatrix},$$

whose condition number is $\|\mathbf{M}\|_2 \cdot \|\mathbf{M}^{-1}\|_2 \approx 24.4945$, and determinant given as $\det(\mathbf{M}) \approx 29$, thus indicating good numerical stability for the inverse transformation.

In a second run of 200 experiments, we lowered the tolerance $\varepsilon = 0$, and did the preconditioning as before. This time, we got 20 out of 200 trials with a positive p-value, although only in three cases, our fit was accepted at $p > 0.05$. The best fit was obtained at $p = 0.536$, showing that the preconditioning works equally well with more complex hierarchical structures due to lower tolerance levels.

This transformation is applied *before* the copula fit, and must be carried through the derivation of predictive densities when obtaining a fit. We omit the simple and obvious changes to the upcoming formulas for simplicity, bearing in mind that actually a linearly transformed version of the data is under investigation, calling for the linear transformation to be inverted for predictions.

As an open issue, however, it remains interesting to find better ways than simple try-and-error to find a preconditioning matrix $\mathbf{A}$ that gives better fits than the plain data would do. Moreover, we believe that this trick may be of independent interest and use in other applications of copula theory, not limited to statistical descriptions of quantum key distribution devices.

 ISBN: 978-1-61208-380-3

IV. PREDICTION OF QBER RATES

Based on a model that describes the relationship between QBER and the environmental quantities, we look for a prediction of the QBER when all the other quantities are known. Having an idea of what values are to be expected, one might suspect an adversary to be present if these values are clearly exceeded. An essential ingredient to find a prediction is the conditional density, as it shows which values are likely in a given situation, that is, we seek the density of QBER conditional on all the other environmental parameters, i.e., the function

$$f(\text{QBER}|\text{TEMP}, \text{HUM}, \text{DUR}, \text{RAD}).$$

Section IV-A describes the general technique to compute the sought density, taking QBER as the n-th variable x_n in the upcoming descriptions. We stress that, however, the method is equivalently applicable to predict any other variable than QBER, too.

A. Computing Conditional Densities via Copulas

In the case where all the marginals and the copula are continuous, it holds for the transformed variables $u_i = F_i^{-1}(x_i)$ by the independence of copula and margins that

$$f(x_1, \dots, x_n) = f_1(x_1) \cdot \ldots \cdot f_n(x_n) \cdot c_n(u_1, \dots, u_n),$$

where $c_n(u_1, \dots, u_n)$ denotes the density of the n-dimensional copula $C_n(u_1, \dots, u_n)$ and f_i denotes the density of the marginal distribution F_i.

Example IV.1. *In the case of independent random variables, the above formula yields $c_n(u_1, \dots, u_n) = 1$, which is the derivative of the independence copula $C_n(u_1, \dots, u_n) = u_1 \cdots u_n$ from Example II.3.*

With this decomposition, the conditional density comes to

$$f(x_n|x_1, \dots, x_{n-1}) = f_n(x_n) \frac{c_n(u_1, \dots, u_n)}{c_{n-1}(u_1, \dots, u_{n-1})} \tag{8}$$

for $u_i = F_i(x_i)$. Using (8) to compute the conditional density requires the lower-dimensional copula density $c_{n-1}(u_1, \dots, u_{n-1})$, excluding the variable u_n (corresponding to the variable x_n of interest). So, computing the conditional density (8) from our full n-dimensional copula model proceeds as follows: let the variable x_i range within $[\underline{x}_i, \overline{x}_i]$, then the $(n-1)$-dimensional marginal density is

$$\begin{aligned} f(x_1, \dots, x_{n-1}) &= \int_{\underline{x}_n}^{\overline{x}_n} f(x_1, \dots, x_n) dx_n \\ &= \int_{\underline{x}_n}^{\overline{x}_n} \prod_{j=1}^{n} f_j(x_j) c_n(F_1(x_1), \dots, F_n(x_n)) dx_n \\ &= [\Delta(\overline{x}_n) - \Delta(\underline{x}_n)] \cdot \prod_{j=1}^{n-1} f_j(x_j) \end{aligned}$$

with

$$\Delta(x) := \frac{\partial^{n-1}}{\partial x_1 \cdots \partial x_{n-1}} C_n(F_1(x_1), \dots, F_{n-1}(x_{n-1}), F_n(x))$$

From this, the sought conditional distribution is immediately found as

$$f(x_n|x_1, \dots, x_{n-1}) = f_n(x_n) \frac{c_n(F_1(x_1), \dots, F_n(x_n))}{\Delta(\overline{x}_n) - \Delta(\underline{x}_n)} \tag{9}$$

Note that the density f_n of the variable of interest can be estimated both parametrical or non-parametrical (e.g., via kernel estimators) while in practice the distribution functions are estimated empirically to avoid additional assumptions.

In a general setting, we first compute the copula density (if the copula at hand is differentiable), whose tedious technicalities may conveniently be handled by a computer algebra system like MATHEMATICA or MAPLE. Again, this procedure simplifies within a smaller family of copulas.

For a n-dimensional Archimedean copula, the density turns out to be

$$c(u_1, \dots, u_n) = (\phi^{-1})^{(n)}(\phi(u_1) + \ldots + \phi(u_n)) \prod_{i=1}^{n} \phi'(u_i)$$

where $(\phi^{-1})^{(n)}(t)$ denotes the n-th derivative of the inverse function $\phi^{-1}(t)$. This can be computed for Gumbel, Frank and Ali-Mikhael-Haq copulas, as for example done in [20], but becomes infeasible for the Gaussian copula considered at the beginning.

In the case of a nested copula, there is no simple closed expression available. One has to compute the derivative of the top level copula that describes the behaviour of all variables together which invokes the chain rule. While this may get complex in the general case, it is still practicable in our case.

In models that involve more levels of sub-copulas than the one considered here, one might use the derivative of $C_{L,1}(C_{L-1,1}, \dots, C_{L-1,n_{L-1}})$ that evaluates to

$$\begin{aligned} \frac{\partial^d C_{L,1}}{\partial u_1 \cdots \partial u_d} = \sum_{i=0}^{d-n_{L-1}} \sum_{k_1,\dots,k_{n_{L-1}}} \Bigg\{ & \frac{\partial^{d-i} C_{L,1}}{\partial C_{L-1,1}^{k_1} \cdots \partial C_{L-1,n_{L-1}}^{k_{n_{L-1}}}} \\ & \times \prod_{r=1}^{n_{L-1}} \sum_{v_1,\dots,v_{k_r}} \frac{\partial^{|v_1|} C_{L-1,r}}{\partial v_1} \cdots \frac{\partial^{|v_{k_r}|} C_{L-1,r}}{\partial v_{k_r}} \Bigg\} \end{aligned}$$

where the outer sum is taken over all integers $k_1, \dots, k_{n_{L-1}}$ that sum up to $d - i$ and satisfy $k_j \leq d_{L-1,j}$ while the inner sum is over partitions $v_1, \dots, v_{k_r}$ of those u_i showing up in the r-th copula at level $L-1$. For more details about this specific case, see [18].

B. Self-Adaptation to Environmental Conditions

For a general description, we relabel the variables and let X_n be the device or performance parameter that we wish to predict based on the known environmental conditions $x_1, \dots, x_{n-1}$. Section IV-C illustrates this for $X_n = \text{QBER}$ and $(X_1, X_2, X_3, X_4) = (\text{DUR}, \text{RAD}, \text{TEMP}, \text{HUM})$.

A prediction of X_n, e.g., the QBER rate given the current environmental conditions, is then given by the conditional expectation or, alternatively, by any value x_n that maximizes expression (9) for $f(x_n|x_1, \dots, x_{n-1})$ for the given values $x_1, \dots, x_{n-1}$. This maximization can be done using standard numerical techniques, whose details are outside our scope here.

Since the indication of an adversary's presence hinges on known performance characteristics, most importantly the QBER rate, it is easy to adapt the respective thresholds to the expected values under the current environmental conditions. Adapting to different conditions then amounts to doing the optimization again under the new configuration.

C. A Worked Example

The density $c(u_1, \ldots, u_5)$ of the top level copula $C_{L,1}$ can be calculated by applying the chin rule. To avoid errors in potentially messy calculations like the following, a computer algebra system may become handy.

The copula C describing our network was found to be

$$\exp\left\{ - \left[\left((-\ln u_1)^{\theta_2} + (-\ln u_2)^{\theta_2} \right)^{\frac{\theta_1}{\theta_2}} + \left[\left((-\ln u_3)^{\theta_4} + (-\ln u_4)^{\theta_4} \right)^{\frac{\theta_3}{\theta_4}} + (-\ln u_5)^{\theta_3} \right]^{\frac{\theta_1}{\theta_3}} \right]^{1/\theta_1} \right\} \tag{10}$$

Generally, it holds

$$\frac{\partial^5 C_{3,1}}{\partial u_1 \cdots \partial u_5} = \frac{\partial^5 C_{3,1}}{\partial^2 C_{2,1} \partial^3 C_{2,2}} \cdot \frac{\partial^2 C_{2,1}}{\partial u_1 \partial u_2} \cdot \frac{\partial^3 C_{2,2}}{\partial^2 C_{1,1} \partial u_5} \cdot \frac{\partial^2 C_{1,1}}{\partial u_3 \partial u_4},$$

where the two most inner derivatives compute as

$$\begin{aligned} \frac{\partial^2 C}{\partial u_1 \partial u_2} &= \frac{1}{u_1 \cdot u_2} (\log(u_1) \cdot \log(u_2))^{\theta - 1} \\ &\cdot \exp\left[- \left((-\log(u_1))^\theta + (-\log(u_2))^\theta \right)^{\frac{1}{\theta}} \right] \\ &\cdot \left((-\log(u_1))^\theta + (-\log(u_2))^\theta \right)^{\frac{1}{\theta} - 2} \\ &\cdot \left(((-\log(u_1))^\theta + (-\log(u_2))^\theta)^{\frac{1}{\theta}} + \theta - 1 \right) \end{aligned} \tag{11}$$

for any two-dimensional Gumbel copula C. Alternatively to this straightforward calculation, the two-dimensional density (11) can be computed directly from the generator function using the chain rule

$$\begin{aligned} c(u_1, u_2) &= \frac{\partial^2}{\partial u_1 \partial u_2} \phi^{-1}(\phi(u_1) + \phi(u_2)) \\ &= - \frac{\phi''(C(u_1, u_2)) \phi'(u_1) \phi'(u_2)}{[\phi'(C(u_1, u_2))]^3} \end{aligned} \tag{12}$$

if both derivatives exist (see also [16]).

To find the expression for $\Delta(x)$ we analogously compute

$$\frac{\partial^4 C_{3,1}}{\partial^1 C_{2,1} \partial^3 C_{2,2}} \cdot \frac{\partial^1 C_{2,1}}{\partial u_2} \cdot \frac{\partial^3 C_{2,2}}{\partial^2 C_{1,1} \partial u_5} \cdot \frac{\partial^2 C_{1,1}}{\partial u_3 \partial u_4} \tag{13}$$

with the third order derivative of a Gumbel copula

$$\begin{aligned} \frac{\partial^3 C}{\partial u_1 \partial u_2 \partial u_3} &= \frac{(-\log(u_1) \cdot \log(u_2) \cdot \log(u_3))^{\theta - 1}}{u_1 \cdot u_2 \cdot u_3} \cdot \exp\left[-z^{\frac{1}{\theta}} \right] \\ &\cdot \left(z^{3/\theta - 3} + 3(\theta - 1) \cdot z^{2/\theta - 3} + (\theta - 1)(2\theta - 1) z^{1/\theta - 3} \right) \end{aligned} \tag{14}$$

where $z = (-\log(u_1))^\theta + (-\log(u_2))^\theta + (-\log(u_3))^\theta$. Again, this density can be computed from the generator function directly if all necessary derivatives exist, yielding

$$\begin{aligned} & \frac{\partial^3}{\partial u_1 \partial u_2 \partial u_3} \phi^{-1} \left(\phi(u_1) + \phi(u_2) + \phi(u_3) \right) \\ &= \phi'(u_1) \phi'(u_2) \phi'(u_3) \frac{3[\phi''(C)]^2 - \phi'''(C) \cdot \phi'(C)}{[\phi'(C)]^5} \end{aligned} \tag{15}$$

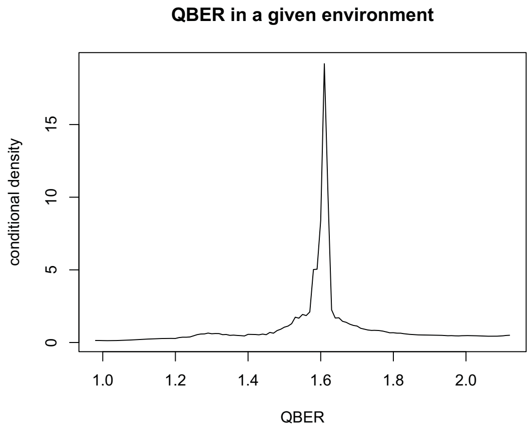

Figure 4. Density of QBER in a known environment

with the abbreviation $\phi(C) = \phi(C(u_1, u_2, u_3))$.

For the quantum network considered here, the conditional density of the QBER displayed in Figure 4 displays a unique maximum of the conditional density around QBER $= 1.61\%$, given typical environmental conditions that represent the current situation: sunshine duration DUR $= 0$s, global radiation RAD $= 0$W/m^2, relative humidity HUM $= 88\%$, and air temperature TEMP $= 14.4$°C. This means that QBER-values lower than 1.14% or higher then 2.07% are unlikely (i.e., these regions have a probability mass of 5% together) and probably arising from the presence of an eavesdropper.
Our analysis has been performed for typical values of the environmental variables, i.e., we set the variable DUR to zero as the sun did typically not shine during the measurement process. Variation of these values does not fundamentally affect out findings as the shape ot the conditional density does not change signifficantly.

V. CONCLUSION

Now, we come back to the initial problem that motivated this entire study. Recall that in a QKD setting, an unnaturally high qubit error rate indicates the presence of an adversary. Conversely, we need an idea about the "natural" rate of qubit errors. Given the conditional density (8) and according to the previous remarks, we can thus obtain a threshold for the qubit error rate that is tailored to the implementation, environment and device, and which can be adapted to changing environmental conditions. The steps are the following:

1) We run the device in a setting where there is no eavesdropper on the line to draw a series of measurements under clean conditions. In particular, we elicit all environmental variables of interest, especially the qubit error rate.
2) We fit a copula model to the so-obtained data $\mathbf{D}$, possibly doing a pre-conditioning (as described in Section III-C) for a statistically and numerically good fit. The fitting can be done using standard statistical software like `R`, using copula-specific libraries like `HAC` [17]. The derivation of the conditional distribution is easy by virtue of computer algebra systems like MATHEMATICA.

3) Having the copula-model, we obtain the conditional distribution (9) of the QBER under all environmental influences. Its maximization gives the currently valid threshold under the present environmental conditions. Speaking differently, this process tells us which values of the QBER are *not* likely enough to occur for a given value of the keyrate.

The respective details of each step have been described in previous Sections, giving examples along the way to illustrate the particular tasks. Nevertheless, the above process remains of generic nature and calls for appropriate instantiation (e.g., different environmental influences such as noisy source and detectors or turbulence structure of the air could be considered).

Once the probability density of the QBER conditional on current working conditions is obtained, it is a simple matter to equip a QKD device with sensory to keep the expected natural QBER rate continuously updated. We stress that this updating is unaffected by the presence of an attacker, unless the intruder manages to steer the environmental conditions in a way s/he likes. Assuming the absence of such an ability, the copula dependency model and its implied predictive distributions are an effective mean to let the devices re-calibrate themselves under the changing working conditions. Next steps in this research direction comprise practical experiments under variable lab conditions to test the quality of QBER adaption in terms of a performance gain over statically configured devices. As an important side-effect, this would also reveal possibilities to attack a QKD line by changing environmental factors. Such an attack has seemingly not been considered in the literature so far.

References

[1] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” Nature, vol. 299, no. 802, 1982, pp. 802–803.

[2] Peev et al., “The SECOQC quantum key distribution network in Vienna,” New Journal of Physics, vol. 11, no. 7, 2009, p. 075001.

[3] K. Lessiak, C. Kollmitzer, S. Schauer, J. Pilz, and S. Rass, “Statistical analysis of QKD networks in real-life environments,” in Proceedings of the Third International Conference on Quantum, Nano and Micro Technologies. IEEE Computer Society, February 2009, pp. 109–114.

[4] K. Lessiak, “Application of generalized linear (mixed) models and nonparametric regression models for the analysis of QKD networks,” Master’s thesis, Universität Klagenfurt, 2010.

[5] T. Schmitt-Manderbach, “Long distance free-space quantum key distribution,” Ph.D. dissertation, Ludwig–Maximilians–University Munich, Faculty of Physics, 2007.

[6] H. Xu, L. Ma, A. Mink, B. Hershman, and X. Tang, “1310-nm quantum key distribution system with up-conversion pump wavelength at 1550 nm,” Optics Express, vol. 15, Jun. 2007, pp. 7247–7260.

[7] M. Li et al., “Measurement-device-independent quantum key distribution with modified coherent state,” Opt. Lett., vol. 39, no. 4, Feb 2014, pp. 880–883.

[8] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, “Experimental demonstration of long-distance continuous-variable quantum key distribution,” Nature Photonics, no. 5, 2013, pp. 378–381. [Online]. Available: http://www.nature.com/nphoton/journal/v7/n5/full/nphoton.2013.63.html [retrieved: September, 2014]

[9] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, “Device-independent security of quantum cryptography against collective attacks,” Physical Review Letters, vol. PRL 98, 230501, no. 1–4, 2007.

[10] Y. Liu et al., “Experimental measurement-device-independent quantum key distribution,” Phys. Rev. Lett., vol. 111, no. 13, 2013, p. 130502. [Online]. Available: http://www.biomedsearch.com/nih/Experimental-Measurement-Device-Independent-Quantum/24116758.html [retrieved: September 2014]

[11] C. Ruican, M. Udrescu, L. Prodan, and M. Vladutiu, “Adaptive vs. self-adaptive parameters for evolving quantum circuits,” in Evolvable Systems: From Biology to Hardware, ser. Lecture Notes in Computer Science, G. Tempesti, A. Tyrrell, and J. Miller, Eds. Springer Berlin Heidelberg, 2010, vol. 6274, pp. 348–359.

[12] C.-J. Lin, C.-H. Chen, and C.-Y. Lee, “A self-adaptive quantum radial basis function network for classification applications,” in Proc. of International Joint Conference on Neural Networks, Vol. 4. IEEE, July 2004, pp. 3263–3268.

[13] A. M. Al-Adilee and O. Nánásiová, “Copula and s-map on a quantum logic.” Inf. Sci., vol. 179, no. 24, 2009, pp. 4199–4207.

[14] P. Embrechts, F. Lindskog, and A. McNeil, Modelling Dependence with Copulas and Applications to Risk Management, Handbook of Heavy Tailed Distributions in Finance, Elsevier, 2001.

[15] D. Kelly, “Using copulas to model dependence in simulation risk assessment,” in Proc. of 2007 ASME International Mechanical Engineering Congress and Exposition. American Society of Mechanical Engineers, 2007, pp. 81–89.

[16] R. Nelsen, An Introuction to Copulas. Springer, 2006.

[17] O. Okhrin and A. Ristig, “Hierarchical archimedean copulae: The HAC package,” Journal of Statistical Software, vol. 58, no. 4, 2014, pp. 1–20. [Online]. Available: http://sfb649.wiwi.hu-berlin.de/papers/pdf/SFB649DP2012-036.pdf [retrieved: September, 2014]

[18] C. Savu and M. Trede, “Hierarchies of Archimedean copulas,” Quantitative Finance, vol. 10, no. 3, February 2010, pp. 295–304.

[19] C. Genest and B. Rémillard, “Validity of the parametric bootstrap for goodness-of-fit testing in semiparametric models,” Annales de l’institut Henri Poincaré (B) Probabilités et Statistiques, vol. 44, no. 6, 2008, pp. 1096–1127. [Online]. Available: http://eudml.org/doc/78005 [retrieved: September, 2014]

[20] C. Savu and M. Trede, “Goodness-of-fit tests parametric families of Archimedean copulas,” Quantitative Finance, vol. 8, no. 2, March 2008, pp. 109–116.

 ISBN: 978-1-61208-380-3