Detecting Trojan-Horse Attacks in Practical QKD via Gaussian Mixture Modeling-Assisted QBER Goodness-of-Fit Analysis

Hong-fu Chou, Heyang Peng, Thang X. Vu, Ilora Maity, Youssouf DRIF, Luis M. Garces-Socarras,
Jorge L. Gonzalez-Rios, Juan Carlos Merlano-Duncan, †Sean Longyu Ma, Symeon Chatzinotas
Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg
†School of Computer Science, The University of Auckland, New Zealand

Abstract—**Quantum key distribution (QKD) offers exceptionally high levels of data security during transmission by using principles of quantum physics. It is renowned for its provable security features. However, a gap between theoretical models and real-world applications, known as quantum hacking, challenges the reliability of QKD networks. Trojan-horse attacks represent a significant threat to the Bob subsystem in QKD, allowing Eve to infer Alice's basis choices through back-reflected pulses. This can compromise security without detection in severe cases, especially when quantum bit error rates (QBER) fall below the abort threshold. The proposed method combines a category-based Gaussian Mixture Model (GMM) with the Kolmogorov-Smirnov test to estimate the posterior QBER distribution and assess risks in practical QKD systems. By processing the QBER, the approach also evaluates the dependability of the QKD scenario. Numerical results are presented using a state-of-the-art point-to-point QKD device operating over optical quantum channels of 1 m, 1 km, and 30 km lengths. The results of the experimental analysis of a 30 km optical link suggest that the QKD device provided prior information to the proposed learner. Consequently, our proposed trustworthy monitor offers a defensive mechanism that identifies potential Eve attacks, effectively mitigating the risk of security vulnerabilities.**

I. Introduction

The deployment of quantum key distribution (QKD) networks in the future and forthcoming scenarios has garnered significant interest due to their potential to provide ultra-secure communication services. Analyzing the current state of critical components in quantum networks enables the ability to link quantum devices across long distances, resulting in significant improvements in communication, network efficiency, and security [1]. The authors in [2] demonstrate the potential for building global quantum networks by transmitting essential information through free-space optical channels (FSO). To attain a state of absolute security, QKD is used as a protocol that, in principle, ensures the confidentiality of information sent between two distant nodes by establishing secure keys. This approach has been extensively studied and documented in the literature, as seen in [3] and [4].

QKD has emerged as an extensively investigated quantum communication system [5]. Long-distance FSO quantum communications have been successfully implemented across very long distances, as shown in [6]. Various experiments have been conducted, such as those presented in [7] and [8]. In the following discourse, we present our methodology, supported by ID Quantique (IDQ), a business based in Switzerland that offers cutting-edge industrial solutions for QKD networks [9]. This technique entails the establishment of a QKD infrastructure using the BB84 communication protocol [10] or a similar invention. The QKD device is usually implemented using the BB84 protocol, but Eve cannot access the key sent in QKD communication. However, ensuring the precise alignment of practical implementations of QKD systems with their corresponding theoretical requirements is challenging. Discrepancies between theory and practice can potentially create vulnerabilities and undermine the integrity of security measures [11].

Trojan-horse attacks have been recognized as a specific risk, primarily targeting the Bob subsystem. The nature of the attack [12] is that Eve employs a method of attack against Bob by transmitting luminous Trojan-horse pulses to ascertain the specific bases Alice chose during the execution of the QKD protocol. The transmission of this information is facilitated by the back-reflected pulses emitted from Alice. In adherence to a general principle, Eve must minimize interference with the authentic quantum signals transmitted from Alice to Bob, as her primary objective is to ascertain the foundation settings. In this hypothetical scenario [12], when Eve successfully achieves correlations over 48% using the key obtained through an identical forward error code, Alice and Bob cannot detect the parameters being attacked. Additionally, the QBER of 5% is significantly lower than the QBER abortion rate of 11%. It may be concluded from this extreme case that the security of the QKD system has been compromised and does not elicit any significant concern, as the percentage to be deducted throughout the process of privacy amplification is 47.8%, a value lower than the extent of Eve's understanding. While Eve continues to interfere, the escalating QBER to the abortion rate leads to the complete loss of the key sequence, while Alice and Bob are compelled to engage in retransmission.

In addition to the interference caused by Eve, a time-invariant quantum channel can also be observed, resulting in a decrease in the key rate reported in the experimental outcomes of the IDQ QKD device when used in long-distance 30km QKD networks. The risks arising from Eve's interference residing in the characteristics of the time-variant quantum channel in QKD networks are considered. This situation

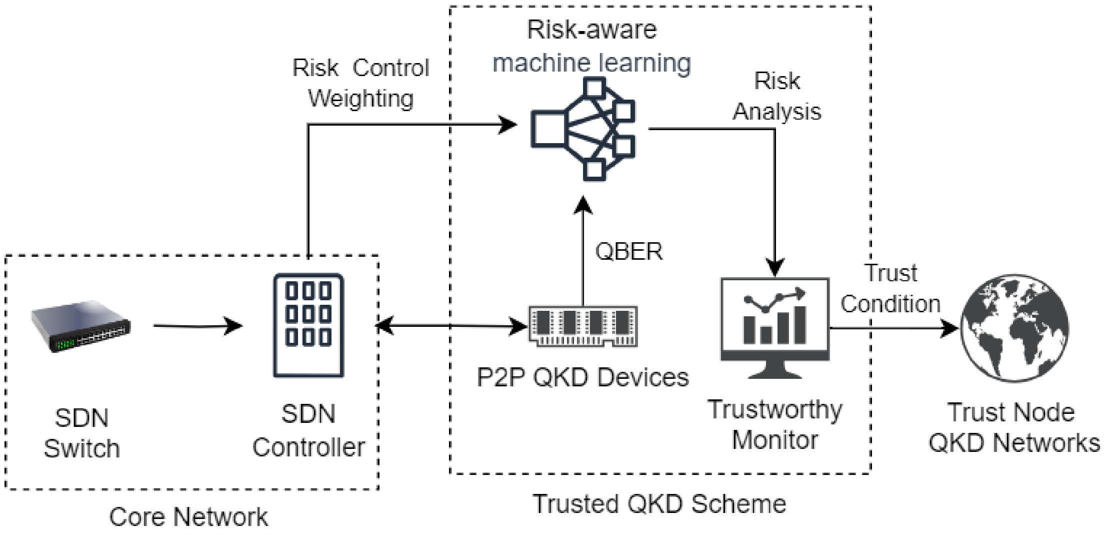

Figure 1: An illustration of the QKD scenario with trustworthy monitor against quantum hacking

poses a certain level of risk contingent upon the QKD key consumption while eavesdropping occurs. As shown in Fig. 1, the risk of quantum hacking can be demonstrated by figuring out a loss function that takes into account what is known about the software-defined network (SDN) controller's assigned traffic, eavesdropping, changes in quantum channel parameters that cause time-varying effects, and what is known about the past from the empirical QBER data. IDQ DV-QKD Cerberus XGR devices obtain the empirical data via the optical quantum channel in our single and multiple campus dark fiber experiments. The primary objective of Trojan-horse detection [13] is to improve the overall reliability of the system and ensure the integrity of the circuits. By emulating the approach taken by detection networks [14], deep learning networks encapsulate the unidentified trigger shape and deviations in decision boundaries introduced by backdoors by acquiring features derived from adversarial patterns and their characteristics. The application of adversarial perturbations to get their imprint is an approach. The introduction of a backdoor alters the decision limits of a network, which are effectively communicated through adversarial perturbations. Because of the approach above, our contributions are summarized as follows:

1) To establish reliable assurance, we initiate risk analysis to provide a trust paradigm that mitigates the gap between theory and practice by considering the potential eavesdropping interference on top of the loopholes of practical concern.
2) The proposed approach involves utilizing the category-based Gaussian Mixture Model (GMM) in conjunction with the Kolmogorov-Smirnov (KS) test for assessing goodness-of-fit. This method aims to estimate the posterior probability distribution of the empirical QBER dataset to evaluate the potential risks associated with practical QKD systems.
3) The deployment of trustworthy QKD networks enables risk awareness and validation of the trust condition [15]. We evaluated Trojan horse attacks in a trusted QKD setup, where Eve's intrusion follows a Poisson process and induces a small, uniformly distributed increase in QBER. Our proposed trustworthy monitor effectively detects these attacks by identifying violations of the trust condition, with sensitivity determined by the defense gate level and risk loss thresholds.

The subsequent sections of this paper are structured as follows. Section II introduces the proposed learner that can learn the QBER distribution of the QKD device. Section III presents the numerical results for the trustworthy QKD scenario to apply the aforementioned risk analysis and the learning procedure. Section IV concludes with a summary of the key insights gained from the study.

II. Category-based GMM-assisted Goodness-of-Fit of QBER estimation for risk measurement

In this section, we provide a novel approach to unsupervised machine learning, specifically designed for the learner denoted $\widehat{\mathbf{Q}} = \lambda(\widehat{\theta})$. The category-based GMM [16] uses statistical tools as an integral component of a data-driven approach. This evaluation procedure entails implementing a method known as soft clustering, where data samples are assigned to distinct groups based on specific criteria, generating a numerical categorization output.

We propose using unsupervised learning techniques to facilitate the model-fitting process as an alternative to the methodology presented in [16]. The selection of the Kolmogorov-Smirnov (KS) criteria is based on its status as the only extensively established goodness-of-fit criterion that exhibits competitiveness when compared to other methods examined in the literature, particularly regarding shift and comparable alternatives. Furthermore, this method allows for the development of straightforward confidence processes and tests. The approach we propose combines the use of the two-sample KS test [17] to assess the similarity of the two samples in terms of their distribution. This technique is employed as a means of presenting an innovative methodology. This is achieved by evaluating the P-value [18] between empirical QBER data and the data generated by the tentative GMM. In [18], the resolution to a well-recognized constraint of the conventional P-value lies in its limited ability to identify deviations occurring at the extreme ends of the distribution. This test is employed to evaluate the goodness of fit and determine the appropriate categorization for new data points when the dataset does not conform well to the present category of GMM cluster distribution. With the core of the Expectation Maximization (EM) algorithm, we present the proposed category-based GMM KS learning to provide the estimated QBER pdf for the aforementioned empirical risk analysis.

As presented in Algorithm 1, we apply this learning methodology as the core of the proposed GMM KS learner $\lambda(\widehat{\theta})$. In the Ensure, the parameter $\widehat{\theta}$ can be obtained as $\{G_s\}_c$. In line 7 and 8, an exhaustive search $T_{max} \times I_{max}$ is performed to fit the empirical data by comparing the similarity between $gmm_s(G_s, c, m)$ and F_s. The GMM parameter $\{G_s\}_c$ is recorded in line 10 along with its corresponding maximum P-value $\{p_s\}_c$. Next, the training phase of the proposed learner is presented in Algorithm 2 using the core of Algorithm 1. As the Input, the empirical training dataset can be partitioned into many folds to establish a suitable correspondence between the two samples; a threshold ς is provided. As indicated in line 7, the purpose of this threshold is to maximize the probability $P(\epsilon = \widehat{\epsilon} \mid \widehat{\mathbf{Q}})$ while minimizing the number of categories. Upon the failure of Algorithm 1 to adequately maintain the desired level of fit, a new category is established at line 10. Finally, the testing phase regarding Algorithm 3 involves performing the same learning as Algorithm 2 and is stated as follows. In lines 6 to 12, the sole distinction lies in the absence of enhanced categories during the test phase. Instead, the focus is on identifying the most suitable match within the pre-existing categories. Following completion of the learning process, the learner performs a thorough and comprehensive search of T_{Test} for each category, as indicated on lines 14 to 17.

Algorithm 1 GMM Model Fitting using EM KS-Test

```
 1: Input: Target dataset $F_s$, GMM parameter $G_s$, number of
    GMM clusters $2, \dots, c_{\max}$, GMM maximum trial number
    $T_{\max}$, EM maximum iteration $I_{\max}$
 2: Output: Distribution set of GMMs $\{G_s\}_c$ and $\{p_s\}_c$ as
    p-values of KS test
 3: Initialize: GMM with random parameter $G_s$
 4: for $c = 2$ to $c_{\max}$ do
 5:     for $m = 1$ to $T_{\max}$ do
 6:         Run EM algorithm to fit $F_s$
 7:         $gmm(G_s, c, m) \leftarrow \mathrm{EM}(F_s, c, G_s, I_{\max})$
 8:         $p_s^{(m)} \leftarrow KS\_test(gmm(G_s, c, m), F_s)$
 9:     end for
10:     $m' \leftarrow \arg\max_{m \in \{1, \dots, T_{\max}\}} p_s^{(m)}$
11:     $\mathrm{gmm}(G_s, c) \leftarrow \mathrm{gmm}(G_s, c, m')$
12:     $\{p_s\}_c \leftarrow p_s^{(m')}$
13: end for
14: return $\{G_s\}_c, \{p_s\}_c$
```

Algorithm 2 Category-based GMM KS-Test Learning in Training Phase

```
 1: Input: Training dataset divided into $K$ folds: $F_1, \dots, F_K$;
    Threshold $\tau$ for KS-test p-value
 2: Output: Category dataset: $\{C_1, \dots, C_H\}$; GMM parameters:
    $\{\{G_s\}_c\}_h$; KS p-values: $\{\{p_s\}_c\}_h$, for $h =
    1, \dots, H$;
 3: Initialize: Set first category $C_1 \leftarrow F_1$, set category index
    $h \leftarrow 1$
 4: for $s = 2$ to $K$ do                         ▷ Process remaining folds
 5:     Run Algorithm 1 on fold $F_s$ with $T_{\max} = T_{\text{training}}$
 6:     Obtain: $\{G_s\}_c \rightarrow \{\{G_s\}_c\}_h$, and $p_s \rightarrow \{\{p_s\}_c\}_h$
 7:     if $\{p_s\}_c > \tau$ then
 8:         Assign $F_s$ to current category: $F_s \rightarrow C_h$
 9:     else
10:         Create new category: $F_s \rightarrow C_{h+1}$
11:         Increment category index: $h \leftarrow h + 1$
12:     end if
13: end for
14: return Category set $\{C_1, \dots, C_h\}$, GMM parameters
    $\{\{G_s\}_c\}_h$, and p-values $\{\{p_s\}_c\}_h$
```

Algorithm 3 Category-based GMM KS-test Learning During Testing Phase

```
 1: Input: Testing folds $F_1, \dots, F_Z$; KS-test threshold $\varsigma$;
    Category datasets $C_1, \dots, C_H$ from training
 2: Output: $\{\{G_s\}_c\}_h$ and $\{\{p_s\}_c\}_h$ for $h = 1, \dots, H$
 3: Initialize: Use training parameters to set $\{\{G_s\}_c\}_h$
 4: for $s = 1, \dots, Z$ do                        ▷ Loop over test folds
 5:     for $h = 1, \dots, H$ do                    ▷ Check each category
 6:         Run Algorithm 1 on $F_s$ using $\{\{G_s\}_c\}_h$ with
    $T_{\max} = T_{\text{Training}}$
 7:         Output: $\{\{G_s\}_c\}_h$ and $\{\{p_s\}_c\}_h$
 8:         if $\{\{p_s\}_c\}_h > \varsigma$ or $h = H$ then
 9:             Assign $F_s \rightarrow C_h$
10:             break
11:         end if
12:     end for
13: end for
14: for $h = 1, \dots, H$ do        ▷ Final category-wise refinement
15:     Run Algorithm 1 on $C_h$ using $\{\{G_s\}_c\}_h$ with $T_{\max} =$
    $T_{\text{Test}}$
16:     Output: updated $\{\{G_s\}_c\}_h$, $\{\{p_s\}_c\}_h$
17: end for
18: return $\{\{G_s\}_c\}_h$ and $\{\{p_s\}_c\}_h$
```

III. Numerical result

A. Trusted QKD Scenario Configuration

The statistical data for the QBER was acquired via the LUQCIA project[1]. This data was gathered using the QNET WEBAPI interface version 1.168 at constant intervals over many months. These data points were used to establish the sample space for our observations.

- The experimental setup for measuring the quantum channel distance consists of three different distances: 1 m, 1 km, and 30 km. The number of QBER experiments $N = \{N_{1m}, N_{1km}, N_{30km}\} = \{57471, 52104, 47768\}$.
- In the context of IDQ QKD devices, if visibility is below 0.9 or QBER exceeds the abortion rate of 11%, it can be shown that Bob is unlikely to receive any raw keys reduced by privacy amplification, leading to a key rate of 0. Eve believes that eavesdropping cannot affect the visibility of data transmission, which is only influenced by the presence of an optical fiber link. The various distance quantum channel experiments can obtain statistical QBER data via IDQ QKD device pairs.
- In the proposed learning scenario, the values of $T_{Training}$ and T_{Test} are determined as 100 and 10000, respectively. The value c_{max} is selected as 15 and 45. The maximum number of iterations of the EM algorithm I_{max} is set to 100.

B. QBER Estimation and Risk Analysis for a Trustworthy Monitor

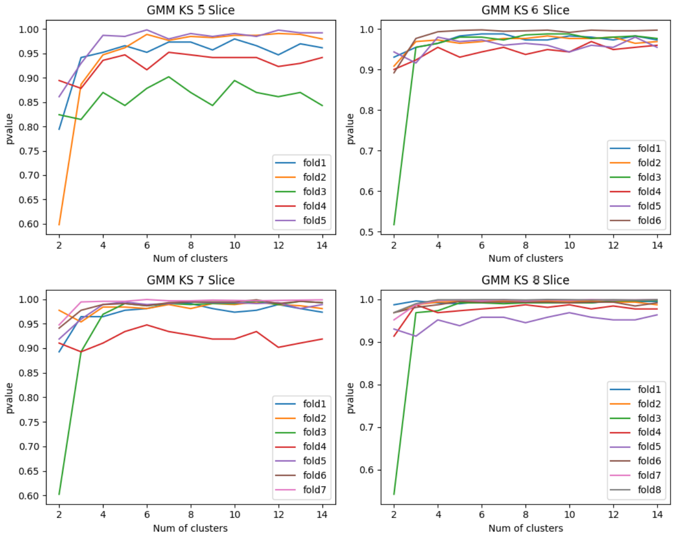

Figure 2: Multiple folders model fitting using Algorithm 2 over the 1 m optical quantum channel

The P-value in Algorithm 2 is shown in Fig. 2, where the value of K is set to 5, 6, 7, and 8, and N is set to N_{1m}. This presentation illustrates the application of GMM fitting to empirical QBER data. In the test phase, cross-validation [19] is a highly effective method to evaluate the performance of the proposed learner. The empirical sample QBER $N = \{N_{1km}, N_{30km}\}$ is divided into four folds. In each cross-validation iteration, one fold is designated as the test set. In contrast, the remaining folds serve as the training set, as illustrated by the P-value in Fig. 3 over 1 kilometer and in Fig. 5 over the 30km optical quantum channel. As shown in Fig. 4 using Algorithm 3, the Akaike Information Criterion (AIC) is utilized to assess the performance of statistical models and determine their efficiency level when applied to a certain data set. The risk analysis assumes that the risk control weighting H_{M_j} follows a normal distribution. In order to demonstrate the effectiveness of the proposed approach, risk control weighting has a mean value that is uniformly

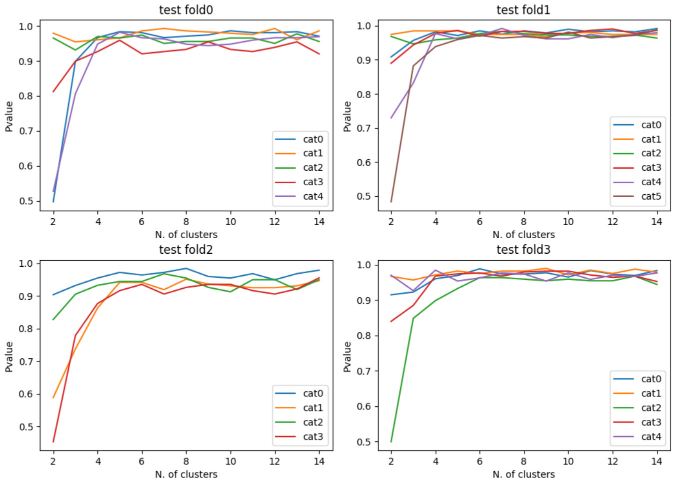

Figure 3: 4-fold cross-validation for Algorithm 3 where $\varsigma = 0.95$ over the 1 km optical quantum channel

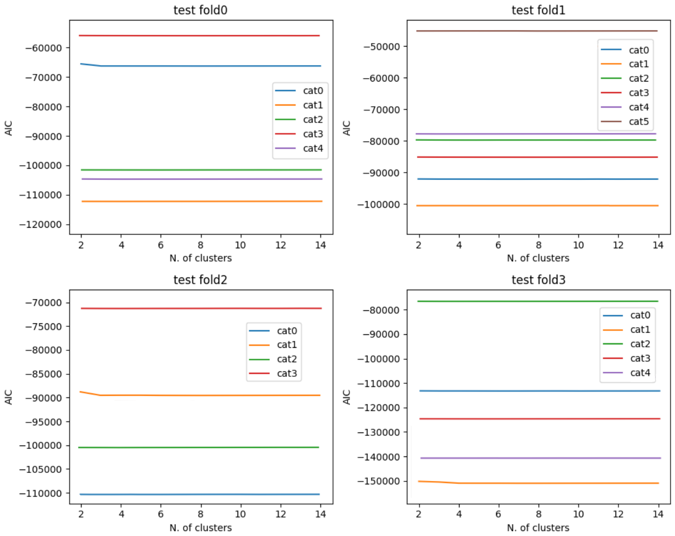

Figure 4: AIC Results of Algorithm 3 where $\varsigma = 0.95$ over the 1 km optical quantum channel

[1] https://www.uni.lu/en/news/a-first-testbed-for-quantum-communication-infrastructure-in-luxembourg/

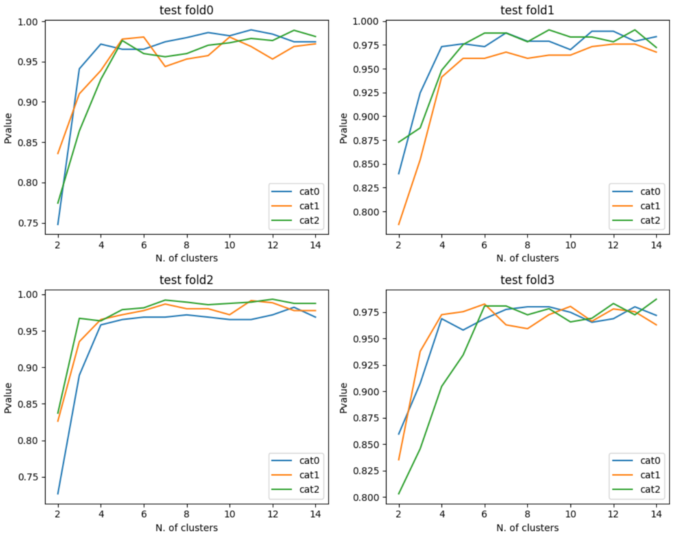

Figure 5: 4-fold cross-validation for Algorithm 3 where $\varsigma = 0.95$ over the 30km optical quantum channel

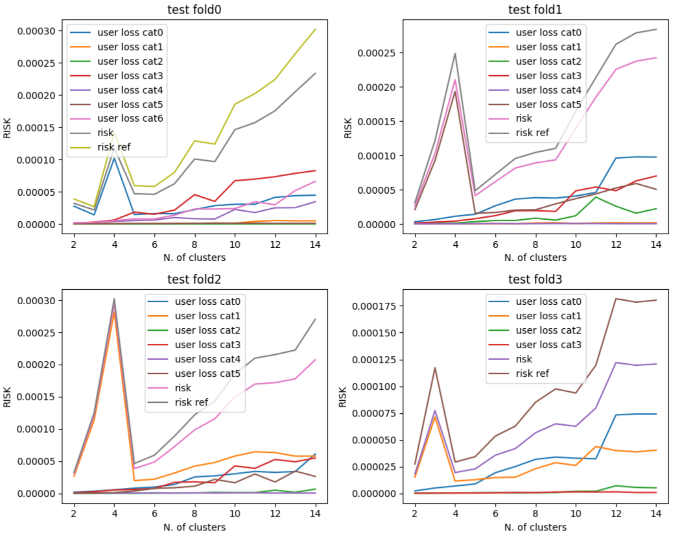

Figure 6: Risk analysis of cross-validation using Algorithm 3 where $\varsigma = 0.95$ and $\rho = 0.05$ over the 1km optical quantum channel

distributed between 0.5 and 1, with a standard deviation equal to the mean value.

Finally, we implement Trojan horse attacks on our trusted QKD scenario, wherein the QKD system is subjected to Eve attacks following a Poisson distribution using the parameter υ_e. Each instance of a Trojan horse attack is assumed to increase the QBER to a uniform distribution ranging from 0.05 to 0.055. The observation of Alice's examination of the defense gate associated with Eve's arrival is intriguing. In Fig. 8 and Fig. 9, the proposed trustworthy monitor can recognize the occurrence of Eve's Trojan horse attacks due to the violation of the trust condition [15]. The value of α has been established using the value of 0.2% according to the maximum value of the risk loss function of 30 km, as shown in Fig. 7. Additionally, Fig. 9 sets υ_e to 4000, and 500 has the identical trend, where the total number of Eve attacks is 10 times compared with 100 times as shown in Fig. 8. It is noteworthy that the risk analysis of Fig. 8 is comparatively greater than Fig. 9, and the proposed QKD scenario can detect Trojan-horse attacks with only the proposition of 0.02%. This discrepancy signifies a distinct sensitivity level in Eve's detection, demonstrating our proposed trustworthy QKD

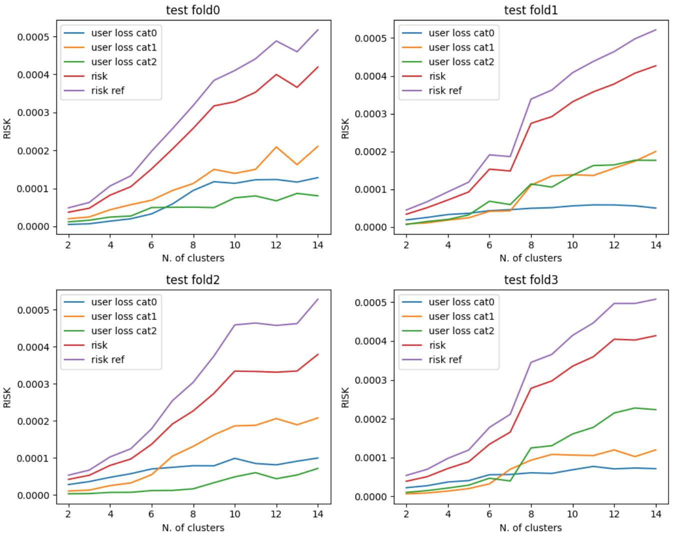

Figure 7: Risk analysis of cross-validation using Algorithm 3 where $\varsigma = 0.95$ and $\rho = 0.05$ over the 30km optical quantum channel

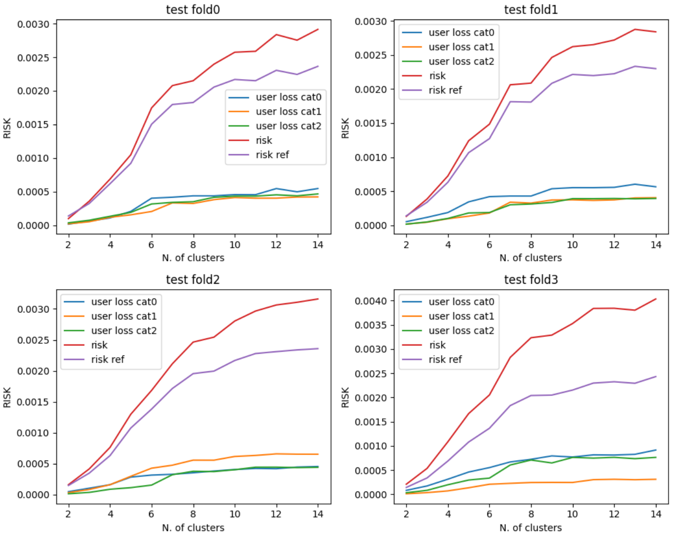

Figure 8: Risk analysis of cross-validation using Algorithm 3 where $\varsigma = 0.95$, $\rho = 0.05$, $\alpha = 0.2\%$ and $\upsilon_e = 500$ with Eve's Trojan-horse attacks over the 30km optical quantum channel

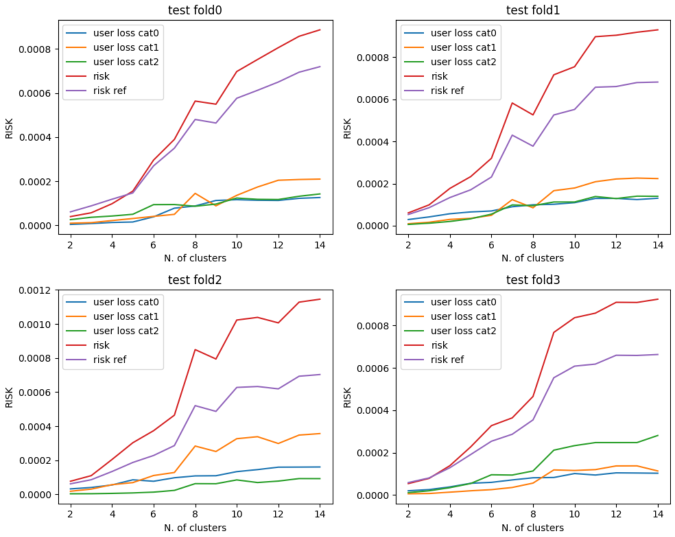

Figure 9: Risk analysis of cross-validation using Algorithm 3 where $\varsigma = 0.95$, $\rho = 0.05$, $\alpha = 0.2\%$ and $\upsilon_e = 4000$ with Eve's Trojan-horse attacks over the 30km optical quantum channel

scenario using the trust condition. Interestingly, the defense gate 0.25% is too high and less sensitive to detect potential Eve attacks, comparing the risk analysis of Fig. 8 and Fig. 9. Consequently, the potential Trojan horse Eve's attack can be successfully detected by our proposed trusted QKD scenario, as shown in the risk difference and loss difference of value between 0.02% and 0.05% in Fig. 7 and Fig. 8. The design of the proposed trustworthy monitor is predominantly determined by the level of defense gate portrayed as obstructing Eve's attacks. We presume that Eve is not acquainted with the time-variant channel effect to preserve generality.

IV. Conclusion and Future Directions

This study is to examine the incorporation of risk-aware machine learning methods [15] into QKD networks, with a particular emphasis on the vulnerability of credentials over a time-variant quantum channel. To accomplish this task, we employ IDQ QKD devices as a means of support. The empirical QBER dataset is effectively estimated by the proposed GMM KS learner, as indicated by the numerical results. The QKD device developed by IDQ is at the forefront of technology and meets the trust condition, making it trustworthy for ultra-secure communication. The simulation can be designed by integrating an SDN controller traffic model with a trust-monitoring component, enabling effective detection of potential Trojan-horse attacks.

Acknowledgment

This work was partially funded by the LUQCIA and LUX4QCI project funded by the Next Generation EU of the European Union, in collaboration with the Department of Media, Connectivity, and Digital Policy (SMC), Luxembourg. This work also has been carried out within the framework of the COST Action 6G-PHYSEC (CA22168), supported by COST (European Cooperation in Science and Technology).

References

[1] L. de Forges de Parny, O. Alibart, J. Debaud, S. Gressani, A. Lagarrigue, A. Martin, A. Metrat, M. Schiavon, T. Troisi, E. Diamanti, P. Gélard, E. Kerstel, S. Tanzilli, and M. V. D. Bossche, "Satellite-based quantum information networks: use cases, architecture, and roadmap," *Communications Physics*, vol. 6, no. 1, jan 2023. [Online]. Available: https://doi.org/10.1038%2Fs42005-022-01123-7

[2] T. P. V., P. A. T., C.-C. Alberto, and T. Moria, "Quantum Key Distribution over FSO: Current Development and Future Perspectives," in *2018 Progress in Electromagnetics Research Symposium (PIERS-Toyama)*, 2018, pp. 1672–1679.

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Mar 2002. [Online]. Available: https://link.aps.org/doi/10.1103/RevModPhys.74.145

[4] D. Mayers, "Unconditional security in quantum cryptography," 2004.

[5] H. Nedasadat, B. Zunaira, M. Robert, N. S. Xin, and H. Lajos, "Satellite-Based Continuous-Variable Quantum Communications: State-of-the-Art and a Predictive Outlook," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 881–919, 2019.

[6] C. Erven, C. Couteau, R. Laflamme, and G. Weihs, "Entangled quantum key distribution over two free-space optical links," *Optics Express*, vol. 16, no. 21, p. 16840, oct 2008. [Online]. Available: https://doi.org/10.1364%2Foe.16.016840

[7] T. Scheidl, R. Ursin, A. Fedrizzi, S. Ramelow, X. song Ma, T. Herbst, R. Prevedel, L. Ratschbacher, J. Kofler, T. Jennewein, and A. Zeilinger, "Feasibility of 300km quantum key distribution with entangled states," *New Journal of Physics*, vol. 11, p. 085002, 2009.

[8] A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein, and A. Zeilinger, "High-fidelity transmission of entanglement over a high-loss free-space channel," *Nature Physics*, vol. 5, no. 6, pp. 389–392, may 2009. [Online]. Available: https://doi.org/10.1038%2Fnphys1255

[9] I. Quantique and R. Extractor, "Quantis," *Quantum number generator*, pp. 2001–2010, 2001.

[10] S.-K. Chong and T. Hwang, "Quantum key agreement protocol based on bb84," *Optics Communications*, vol. 283, no. 6, pp. 1192–1195, 2010.

[11] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, "Attacks on practical quantum key distribution systems (and how to prevent them)," *Contemporary Physics*, vol. 57, no. 3, pp. 366–387, 2016.

[12] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, "Risk Analysis of Trojan-Horse Attacks on Practical Quantum Key Distribution Systems," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 168–177, 2015.

[13] R. Naveenkumar, N. Sivamangai, A. Napolean, and V. Janani, "A Survey on Recent Detection Methods of the Hardware Trojans," in *2021 3rd International Conference on Signal Processing and Communication (ICPSC)*, 2021, pp. 139–143.

[14] X. Zhang, R. Gupta, A. Mian, N. Rahnavard, and M. Shah, "Cassandra: Detecting trojaned networks from adversarial perturbations," *IEEE Access*, vol. 9, pp. 135 856–135 867, 2021.

[15] H.-f. Chou, T. X. Vu, I. Maity, L. M. Garces-Socarras, J. L. Gonzalez-Rios, J. C. Merlano-Duncan, S. L. Ma, S. Chatzinotas, and B. Ottersten, "Empirical risk-aware machine learning on trojan-horse detection for trusted quantum key distribution networks," *arXiv preprint arXiv:2401.14622*, 2024.

[16] H.-C. Yan, J.-H. Zhou, and C. K. Pang, "Gaussian Mixture Model Using Semisupervised Learning for Probabilistic Fault Diagnosis Under New Data Categories," *IEEE Transactions on Instrumentation and Measurement*, vol. 66, no. 4, pp. 723–733, 2017.

[17] V. W. Berger and Y. Zhou, "Kolmogorov–smirnov test: Overview," *Wiley statsref: Statistics reference online*, 2014.

[18] A. Moscovich-Eiger, B. Nadler, and C. Spiegelman, "The Calibrated Kolmogorov-Smirnov Test," *arXiv preprint arXiv:1311.3190*, vol. 65, pp. 694–706, 2013.

[19] C. Schaffer, "Selecting a classification method by cross-validation," *Machine learning*, vol. 13, pp. 135–143, 1993.