applied sciences

IMPACT FACTOR 2.5

CITESCORE 5.5

Article

A Hybrid Quantum–Classical Neural Network Framework for the Detection of Quantum Hacking Attacks in CVQKD

Xinglin He, Jiaxun Xiao and Xuanli Lyu

Special Issue

Quantum Communication and Applications

Edited by

Dr. André Nuno Carvalho Souto and Dr. Nikola Paunkovic

MDPI

https://doi.org/10.3390/app16062793

applied sciences

MDPI

Article

A Hybrid Quantum–Classical Neural Network Framework for the Detection of Quantum Hacking Attacks in CVQKD

Xinglin He [1], Jiaxun Xiao [2] and Xuanli Lyu [2,*]

[1] School of Computer Science and Engineering, Central South University, Changsha 410083, China; 224711081@csu.edu.cn
[2] School of Electronic Information, Central South University, Changsha 410083, China; xiaojiaxun@csu.edu.cn
* Correspondence: 234711009@csu.edu.cn

Abstract

The security of continuous-variable quantum key distribution (CVQKD) systems faces severe challenges from quantum hacking attacks in practical deployments. This paper proposes a novel hybrid quantum-classical neural network (HQCNN) architecture for the detection of quantum hacking attacks. This architecture employs a convolutional neural network (CNN) to extract features from raw pulse signals at the receiver and to reduce spatial dimensionality. Subsequently, the extracted features are mapped into a high-dimensional Hilbert space via angle encoding, and a variational quantum circuit (VQC) is utilized as the core classifier for discrimination. In five-class classification experiments involving local oscillator intensity attacks (LOIA), calibration attacks, saturation attacks, hybrid attacks, and the no-attack state, the HQCNN achieves an overall accuracy of 93%, representing a 6% improvement over the classical residual network (ResNet). In addition, the proposed HQCNN architecture exhibits a significant advantage in parameter efficiency compared with classical deep neural networks. This study provides an efficient intelligent detection scheme for enhancing the practical security of CVQKD systems.

Keywords: continuous-variable quantum key distribution; detection of quantum hacking attacks; hybrid quantum-classical neural network; variational quantum circuit

1. Introduction

Leveraging the Heisenberg uncertainty principle [1] and the quantum no-cloning theorem [2], quantum key distribution (QKD) achieves theoretically unconditional security. QKD can be classified into discrete-variable quantum key distribution (DVQKD) [3–5] and CVQKD [6–8]. In practical applications, DVQKD relies heavily on high-performance single-photon sources and detectors and suffers from significant signal attenuation and noise limitations at long distances. By contrast, CVQKD encodes information using continuous variables, offering higher fault tolerance and improved long-distance transmission capability. Among various CVQKD implementations, the Gaussian modulated coherent state (GMCS) protocol [6] is one of the most widely adopted and promising schemes. GMCS-CVQKD encodes key information into the coherent components of quantum states via Gaussian modulation of the optical field, thereby mitigating the impact of channel loss and noise on system performance and enabling long-distance transmission over existing fiber networks. However, discrepancies between theoretical assumptions and imperfect practical physical devices provide exploitable opportunities for an eavesdropper, Eve. The practical

Academic Editors: Nikola Paunkovic and André Nuno Carvalho Souto

Received: 2 February 2026
Revised: 11 March 2026
Accepted: 12 March 2026
Published: 14 March 2026

deployment of GMCS-CVQKD systems is significantly hindered by security loopholes at the level of physical implementation.

Among the numerous attack strategies, quantum hacking attacks targeting the vulnerabilities of CVQKD systems have emerged incessantly. The LOIA [9] exploits fluctuations in strong local oscillator pulses to disrupt the shot noise estimation at the receiver, Bob. Calibration attacks [10] take advantage of parameter calibration procedures during system initialization or operation to induce Bob to adopt tampered noise reference values. Saturation attacks [11] exploit the nonlinear response of detectors outside their linear operating regime to covertly extract information. Hybrid attacks, formed by combining multiple individual attacks such as intercept-resend attacks [12,13] and homodyne detector blinding attacks [14], exhibit enhanced stealth and destructiveness, rendering traditional single-defense strategies ineffective.

To address the aforementioned security threats, early studies primarily relied on hardware-based approaches such as real-time parameter estimation and physical filtering. However, hardware-based solutions are often constrained by specific physical vulnerabilities and lack sufficient flexibility and robustness when confronting complex quantum hacking attacks, such as hybrid attacks. In recent years, models for the detection of quantum hacking attacks based on machine learning (ML) have attracted widespread attention due to their nonlinear fitting capabilities. Researchers have achieved the identification of various quantum hacking attacks by constructing models such as artificial neural network (ANN) [15] and support vector machine (SVM) [16,17]. Nevertheless, as the key rate of CVQKD systems continues to increase, the limitations of classical ML approaches have become increasingly evident: the large number of parameters in deep models incurs excessive computational overhead, making it difficult to meet the stringent real-time detection requirements of embedded systems.

Meanwhile, the emergence of quantum machine learning (QML) [18,19] has provided new perspectives for overcoming the aforementioned bottlenecks. By exploiting the efficient representational capacity of VQC [20,21] in Hilbert space, QML can characterize complex distribution features with a relatively small number of tunable parameters. Extending this paradigm, the HQCNN framework organically integrates the mature strengths of classical ML in multidimensional feature processing with the nonlinear representational power of VQC in Hilbert space, thereby demonstrating the dual advantages of high accuracy and lightweight design.

Although HQCNN has achieved promising progress in multiple application domains, its application to the detection of quantum hacking attacks in CVQKD systems remains at an early stage, leaving a clear academic gap. On this basis, this paper proposes a HQCNN-based framework for the detection of quantum hacking attacks in CVQKD systems. Through the coordinated use of quantum and classical computational capabilities, the framework fills a key technical gap in quantum hacking defense and facilitates the construction of practically secure CVQKD systems.

The main contributions of this paper are summarized as follows:

A novel HQCNN architecture for the detection of quantum hacking attacks is proposed, in which classical CNN layers are employed to perform multidimensional feature extraction and spatial dimensionality reduction on the raw pulse signals received at Bob's side. Subsequently, the extracted feature vectors are encoded into quantum states, and a VQC is utilized as the core classifier for efficient identification.

This study conducts five-class classification experiments on a dataset simulating the operational environment of practical CVQKD systems, covering LOIA, calibration attacks, saturation attacks, hybrid attacks, and the no-attack state. Experimental results demonstrate that the proposed HQCNN framework achieves an overall accuracy of 93% on the test

dataset, requiring fewer model parameters than ResNet while realizing a 6% improvement in accuracy.

The remainder of this paper is organized as follows. Section 2 reviews quantum hacking attack defenses in GMCS-CVQKD systems and related studies on HQCNNs. Section 3 elaborates on the theoretical foundations of this work. Section 4 presents the proposed HQCNN architecture in detail. Section 5 reports the experimental setup and performance analysis. Section 6 concludes the paper.

2. Related Work

2.1. Detection of Quantum Hacking Attacks in CVQKD

Practical quantum communication systems are constrained by the non-ideal properties of hardware components. These limitations lead to inevitable implementation flaws and technical vulnerabilities. Such gaps leave the system susceptible to quantum hacking attacks. In the practical operating environment of GMCS-CVQKD, common quantum hacking attacks include intercept-resend attacks, LOIA, calibration attacks, saturation attacks, and others.

Early defense strategies primarily focused on real-time monitoring and adjustment of critical physical parameters. To counter LOIA, P. Jouguet et al. [10] proposed introducing a beam splitter in conjunction with a monitoring photodiode to real-time correct shot-noise estimation deviations caused by local oscillator power fluctuations. X. C. Ma et al. [22] proposed that legitimate participants could adjust the local oscillator intensity to an optimal value to counter Eve's potential attacks on the local oscillator. However, these methods are typically effective against only a single specific attack, and traditional defense strategies are prone to failure when confronted with hybrid attacks or covert parameter compensation strategies employed by Eve.

To enhance the flexibility and robustness of detection systems, the research community has begun to explore attack detection algorithms based on ML and deep learning (DL). ML is capable of automatically extracting latent attack features from complex high-dimensional measurement data. Early studies primarily employed ANN and SVM. In 2020, Mao et al. [15] established a generic model for the detection of attacks in CVQKD by analyzing the effects of different attacks on pulse characteristics and constructing feature vectors as inputs to an ANN. More recently, DL has gained prominence due to its superior ability to model nonlinearities and temporal correlations. In 2022, Du et al. [17] proposed an attack detection scheme based on long short-term memory, which enabled the identification of various quantum hacking attacks. In 2025, Iqbal et al. [23] developed a framework based on a deep neural network (DNN) to distinguish quantum hacking attacks from system faults, thereby enhancing the reliability of anomaly identification in practical CVQKD deployments.

Although DL-based approaches significantly raise the upper bound of defense performance, they still face the challenge of a trade-off between resource consumption and real-time requirements in practical deployment. High-performance deep neural networks typically contain a massive number of trainable parameters, which not only increases training costs but also results in high inference latency.

In 2026, Li et al. [24] proposed a generic CVQKD attack detection scheme based on a quantum neural network (QNN), in which classical data acquired by the system are encoded into quantum states and a QNN is trained to perform binary classification between normal and attacked signals. However, this binary classification paradigm exhibits limitations in complex practical scenarios, as the model's generalization performance is constrained when confronted with unknown disturbances or novel hybrid attacks governed by different physical mechanisms.

2.2. HQCNNs

HQCNNs are well-suited for the noisy intermediate-scale quantum (NISQ) era, as they combine the potential advantages of quantum computing with mature classical computing techniques to enhance overall computational efficiency and accuracy. To fully exploit the acceleration capability of quantum computing for specific problems, hybrid quantum-classical algorithms divide the overall computational task into classical and quantum components. The quantum component focuses on particular computational tasks, leveraging the advantages of quantum algorithms to achieve quantum efficiency in problems such as solving linear systems of equations. The remaining tasks are handled by classical computers, including data preprocessing, parameter updating, and optimization feedback for trainable quantum circuits. To date, hybrid quantum-classical algorithms have demonstrated strong practicality and significant development potential across multiple application domains, including QML, quantum combinatorial optimization [25], and quantum chemistry [26].

In HQCNN architectures, hybridity is often manifested as partial quantization of classical neural network models, whereby quantum circuits are introduced to enhance or replace specific layers while preserving the overall classical framework. By deploying quantum circuit layers at different positions within the network, distinct functions can be realized according to task requirements. For example, quantum circuit layers can be used for feature extraction, embedded within hidden-layer structures, or incorporated into the classification decision stage. During feature extraction, specifically designed quantum circuits can map image pixel values or signal features into the state space of qubits [27]. When embedded between the hidden layers of a classical neural network, quantum circuit layers function analogously to classical hidden layers, while exploiting quantum superposition and entanglement to perform complex nonlinear transformations in higher-dimensional spaces [28]. In the output section of the network, the quantum circuit layer can also generate probability distributions for various classes through quantum state measurements, thereby accomplishing the classification task [29].

Owing to their potential to outperform classical methods in solving complex problems, HQCNNs have attracted extensive attention in recent years. Fan et al. [30] further investigated the incorporation of quantum layers into a conventional CNN for large-scale image data processing, demonstrating that this hybrid architecture can significantly reduce computational resource requirements while achieving efficiency comparable to or even exceeding that of a pure CNN. In addition, studies by Bokhan et al. [31] indicate that models combining quantum convolutional layers with classical learning algorithms can effectively handle high-dimensional image data in multiclass image classification tasks. With regard to architecture optimization of HQCNNs, Li et al. [25] proposed a quantum architecture search framework based on Monte Carlo tree search (MCTS) to automatically identify simple and efficient quantum circuits from a vast space of quantum gate combinations.

3. Basic Preliminaries

3.1. Basic Principles of CVQKD

The GMCS protocol is currently the most widely adopted CVQKD protocol, where Gaussian states refer to a class of quantum states whose characteristic functions and Wigner functions both follow Gaussian distributions in phase space. Owing to the relative ease of conducting theoretical and experimental studies based on Gaussian models, most existing CVQKD techniques rely on Gaussian states, Gaussian operations, and Gaussian measurements [32].

A typical GMCS-CVQKD protocol, as illustrated in Figure 1, mainly consists of quantum state modulation, quantum channel transmission, coherent measurement, and classical data post-processing. At the transmitter, Alice, a laser generates a coherent light source,

which is split into a signal beam and a local oscillator. The signal beam passes through an amplitude modulator (AM) and a phase modulator (PM), where independent Gaussian random variables $x, p \sim N(0, V_A)$, are applied to two orthogonal quadratures to prepare a Gaussian-modulated coherent state $|\alpha\rangle = |x + ip\rangle$. The modulated signal beam and the local oscillator are polarization-multiplexed and injected into a quantum channel that may be eavesdropped on by Eve, and then transmitted to Bob. The channel can be abstracted as a Gaussian channel characterized by a transmission efficiency T and excess noise ξ, whose input–output relationship can be expressed as

$$X_B = \sqrt{T}X_A + N_e. \quad (1)$$

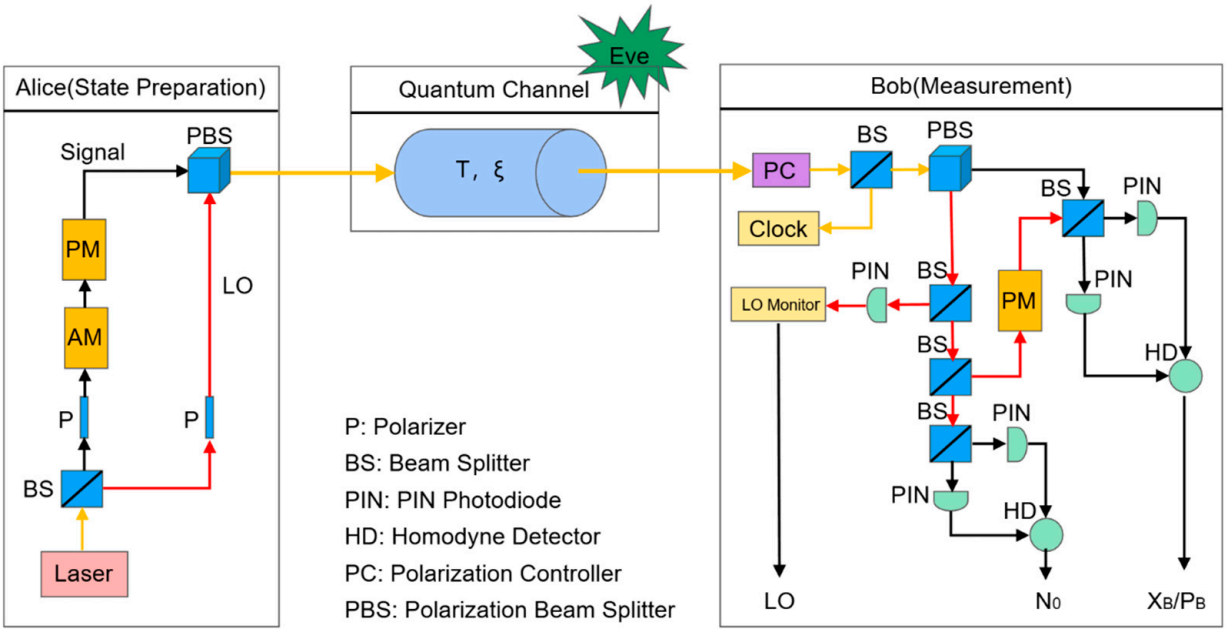

Figure 1. Schematic diagram of the GMCS-CVQKD protocol.

Here, N_e denotes the equivalent noise term composed of vacuum noise and excess noise. Throughout this work, all noise sources are characterized by the variance of the quadrature variables and normalized to the shot-noise unit N_0. At the receiver Bob, the signal beam first passes through a polarization controller (PC) to compensate for polarization drift introduced by the channel, then interferes with the local oscillator at a 50:50 beam splitter, and the selected quadrature X or P is measured using a balanced homodyne detector. During the measurement, a portion of the local oscillator is tapped and monitored in real time by a PIN photodiode to measure the shot-noise unit N_0. This method of shot-noise monitoring does not adversely affect the actual key transmission rate or the normal communication functionality of the system. After completing the quantum measurements, Bob informs Alice of which quadrature component was measured for each pulse, and Alice discards the irrelevant data. The classical data post-processing stage includes parameter estimation, information reconciliation, and privacy amplification. Ultimately, Alice and Bob obtain an information-theoretically secure shared key.

3.2. CVQKD Quantum Hacking Attacks

This section systematically presents the fundamental principles of several typical attack strategies, including LOIA, calibration attacks, saturation attacks, and a hybrid attack scheme. In this study, the parameters for quantum hacking attacks were set to fixed representative values, following the typical attack models described in [15,17], to establish a rigorous benchmark for the proposed HQCNN. These values represent high-

threat scenarios where the attack is subtle enough to evade traditional threshold-based detection but remains physically significant. While fixed parameters were used for initial training, the CNN layers are designed to robustly extract spatial features that capture the invariant statistical signatures, e.g., nonlinear distortion patterns, intrinsic to the attack mechanism, rather than being tied to specific parameter magnitudes.

- LOIA;

In a LOIA, Eve exploits the co-propagation of the signal and local oscillator in the quantum channel to manipulate the local oscillator intensity at the receiver, thereby interfering with Bob's estimation of system noise parameters [33,34]. To characterize Eve's manipulation, a local oscillator intensity scaling factor $k(0 < k < 1)$ is introduced to represent the proportional scaling of the local oscillator power received by Bob relative to the normal case. Assuming that Eve applies the same scaling factor n to all local oscillator pulses, the variance of a single measurement outcome at Bob's side can be expressed as

$$V_B^{LOIA} = kT(V_A + \xi)N_0 + kN_0 + V_{el}. \tag{2}$$

Here, V_A denotes Alice's modulation variance, ξ represents the total excess noise introduced by the channel, including the contribution from Eve's Gaussian collective attack, and V_{el} is the electronic noise variance at the receiver. Meanwhile, since the calibration of shot noise intrinsically depends on the local oscillator power, attenuation of the local oscillator intensity leads to a rescaling of the effective shot-noise measurement at Bob's side, which can be expressed as

$$N_0^{LOIA} = kN_0. \tag{3}$$

- Calibration Attack;

In a calibration attack, Eve exploits the procedures for calibrating shot noise and system gain before or during the operation of a CVQKD system to induce Bob to obtain a tampered shot-noise reference value. Let the shot-noise variance under ideal conditions be denoted as N_0. Under Eve's attack, the calibration value actually used by Bob can be expressed as

$$N_0^{cal} = \alpha N_0, \tag{4}$$

where α denotes the calibration bias coefficient introduced by Eve. In the subsequent key distribution stage, Bob utilizes N_0^{cal} to normalize the measured data, and the equivalent variance of the measurement results can be expressed as

$$V_B^{cal} = \frac{TV_A + 1 + T\xi}{\alpha}. \tag{5}$$

- Saturation Attack;

In a saturation attack, Eve exploits the practical limitation that the balanced homodyne detector at Bob's side has a finite linear response range. By injecting an optical signal with a high-amplitude offset into the receiver, she drives the detector into a nonlinear or even saturated regime. Let the linear response range of the detector be $[-X_{sat}, X_{sat}]$, then the actual output measured by Bob can be modeled as

$$X_B^{sat} = \begin{cases} X_B, & |X_B| \leq X_{sat}, \\ sgn(X_B)X_{sat}, & |X_B| > X_{sat}. \end{cases} \tag{6}$$

Under saturation conditions, the statistical variance of Bob's measurement outcomes will be compressed, i.e.,

$$V_B^{sat}\left(X_B^{sat}\right) < V_B(X_B) = TV_A + 1 + T\xi. \tag{7}$$

- Hybrid Attack;

In a hybrid attack, Eve combines a full intercept–resend attack with the injection of additional optical pulses to launch a joint attack against the CVQKD system. Eve first measures Alice's signal states and reconstructs the signal pulses, while superimposing additional optical pulses onto the resent signals that share the same temporal width and repetition rate as the original pulses but differ in wavelength. Owing to the wavelength-dependent response of the optical components at Bob's receiver, these extra pulses can induce a significant direct-current offset in the homodyne detector and drive it toward saturation without triggering anomaly monitoring. This offset can be expressed as

$$D_{ext} = \sqrt{\eta/I_{LO}}(1 - 2T_{ext})I_{ext}. \tag{8}$$

Here, η represents the detection efficiency of the homodyne detector. T_{ext} and I_{ext} denote the overall transmittance of Bob's side and the average photon number of the additional pulses. D_{ext} is expressed in units of $\sqrt{N_0}$. Under this attack, the total excess noise of the system can be expressed as

$$\xi_{hyb} = \xi + \xi_{IR} + \xi_{ext}. \tag{9}$$

Within this expression, $\xi_{IR} = 2N_0$ represents the noise introduced by the intercept-resend attack, while ξ_{ext} denotes the supplementary noise caused by the additional optical pulses, the magnitude of which is directly correlated with I_{ext}.

3.3. VQC

A typical VQC consists of three functional components: data encoding, an ansatz, and quantum measurement. In our architecture, these components are integrated into a hybrid framework to process features extracted by a classical CNN.

The encoding layer, or feature map, transforms classical data $x \in R^n$ into a high-dimensional quantum Hilbert space. Based on our implementation, we employ Angle Embedding with R_y rotations. For a classical input vector x, the state is prepared by applying a unitary transformation $U_{enc}(x)$ to the initial state $|0\rangle^{\otimes n}$:

$$|\psi(x)\rangle = U_{enc}(x)|0\rangle^{\otimes n} = \bigotimes_{j=1}^{n} R_y(x_j)|0\rangle_j, \tag{10}$$

where $R_y(\theta) = \exp(-i\theta\sigma_y/2)$ represents a rotation around the y-axis of the Bloch sphere. To enhance expressivity, we utilize a data re-uploading [35] strategy, where this encoding is repeated across $L = 4$ layers within the circuit.

The ansatz $U(\theta)$ is a trainable quantum circuit consisting of parameterized gates that capture correlations between features. We utilize the Strongly Entangling Layers architecture. This ansatz combines single-qubit rotations $R(\alpha, \beta, \gamma)$ and periodic entangling gates controlled-NOTs (CNOTs) to achieve high expressivity:

$$|\psi(x, \theta)\rangle = \prod_{l=1}^{L}[U_{ent} \cdot U_{rot}(\theta_l)]|\psi(x)\rangle, \tag{11}$$

where θ_l denotes the set of trainable parameters in layer l, and U_{ent} represents the arrangement of CNOT gates that generate multi-qubit entanglement across n qubit registers.

To retrieve classical information from the quantum state, we perform measurements in the computational basis. The output of the QNN is the expectation value of the Pauli-Z operator $\hat{\sigma}_z$ for each qubit:

$$y_i = \langle \psi(x,\theta) | \hat{\sigma}_{z,i} | \psi(x,\theta) \rangle, \; i \in \{1, \ldots, n\}. \tag{12}$$

The predictive output of the model is obtained by further processing these measured expectation values through subsequent classical layers.

4. Proposed Method

4.1. HQCNN Integration

The proposed HQCNN framework operates on feature representations extracted from this classical processing stage rather than directly interacting with the optical quantum states. Therefore, the HQCNN module can be implemented as an additional security monitoring unit within the receiver-side data processing pipeline.

From a system architecture perspective, the attack detection module can be deployed in parallel with the classical post-processing procedures, such as parameter estimation and key distillation. Since the HQCNN processes compressed feature vectors rather than raw high-rate signal streams, the computational overhead is relatively small and does not interfere with the key generation process.

Regarding the inference mode, the proposed framework assumes that the trained HQCNN model performs near-real-time inference during system operation to monitor potential quantum hacking attacks. Model training can be performed offline using labeled datasets obtained from experimental measurements or simulated attack scenarios. Once trained, the model can be deployed as an online monitoring tool that continuously analyzes system features.

4.2. Overall System Design

The CVQKD attack detection scheme based on a HQCNN proposed in this study is illustrated in Figure 2. The scheme aims to achieve accurate identification of multiple attack patterns by combining the efficient feature extraction capability of classical computation with the nonlinear representational advantages of quantum computation.

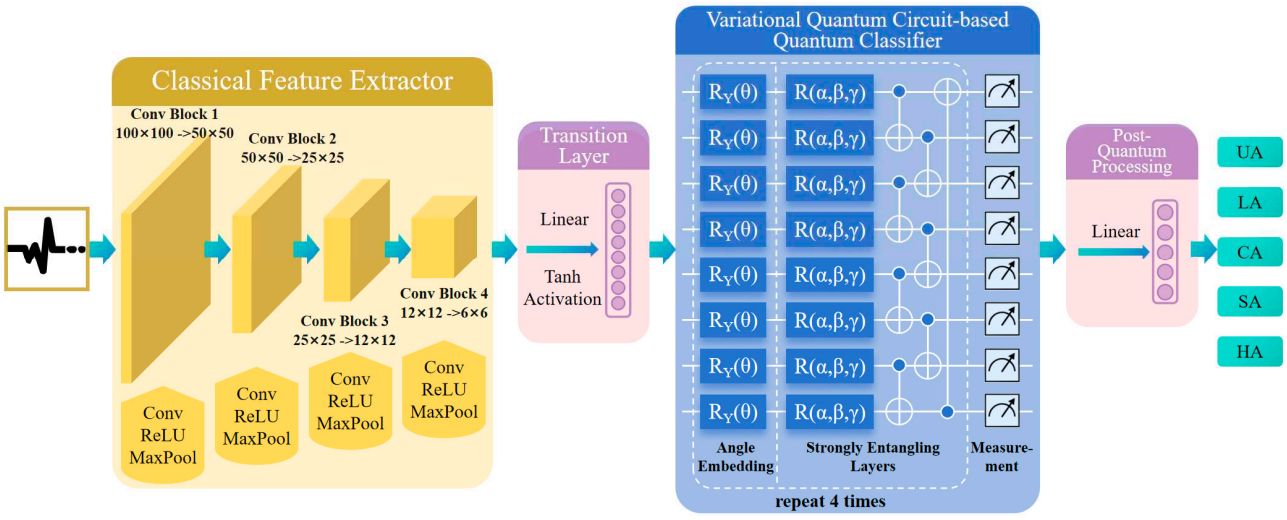

Figure 2. Schematic diagram of the proposed HQCNN framework for the detection of quantum hacking attacks in CVQKD systems.

Specifically, the classical convolutional module leverages its strong local receptive capability to efficiently identify statistical patterns of attack features from massive noise, compressing high-dimensional physical signals into highly representative low-dimensional abstract features. The transition layer serves as a bridge between the high-dimensional classical feature space and the bounded quantum Hilbert space. The core function of the VQC is nonlinear spatial mapping and correlation mining to construct decision boundaries. By exploiting qubit superposition and entanglement, the quantum circuit maps features into an exponentially large Hilbert space, where previously ambiguous attack boundaries are stretched and rendered distinguishable. The post-quantum processing layer effectively aggregates the information captured in quantum states and projects it onto classification logits, thereby determining the predicted probability distribution over attack types.

4.3. Classical CNN-Based Feature Extraction

To enable the CNN to capture the statistical characteristics of pulse sequences in a CVQKD system, the original one-dimensional physical measurement values must first be tensorized. The Q one-dimensional pulse measurements contained in each data block received by Bob are reconstructed according to their temporal order into a $\lceil\sqrt{Q}\rceil \times \lfloor\sqrt{Q}\rfloor$ two-dimensional feature map. This transformation introduces spatial adjacency between pulses previously separated by $\sqrt{Q}$ intervals in the time domain, but it does not create spurious correlations. Instead, it allows the network to simultaneously capture short-term pulse-to-pulse noise and long-term system drifts, such as phase or polarization drifts over hundreds of pulses. This multi-scale perspective is physically relevant for CVQKD, where attack patterns often manifest as slow deviations in the system's noise floor. To match the input range of the neural network and eliminate the influence of physical units, a normalization strategy is adopted to map the amplitude distribution of the original pulses to the $[0,\ 1]$ interval.

The reconstructed two-dimensional feature maps are fed into the deep convolutional module, where abstract feature extraction is achieved by increasing the number of channels while reducing the feature map resolution. The model is designed with four progressive convolutional layers with 32, 64, 128, and 256 channels, respectively, and all convolutional layers employ 3×3 kernels. The ReLU activation function applied after each convolutional layer introduces nonlinear representational capability. The proposed four-layer structure facilitates hierarchical feature extraction: the initial 32 and 64 channels are dedicated to identifying local statistical variances and shot-noise characteristics, whereas the subsequent 128 and 256 channels consolidate these primary features into high-level abstractions of hacking attacks, such as the subtle intensity scaling in LOIA and the nonlinear clipping in saturation attacks. Furthermore, this depth ensures sufficient nonlinear mapping before the transition layer, which is crucial for reducing the high-dimensional physical pulses into a compact feature vector compatible with the limited qubit space of the VQC.

The feature passes through a transition layer before flowing to the VQC. This layer first compresses the high-dimensional classical feature vectors via a linear layer to match the dimensionality of the finite qubit space, and then constrains their values to the range $[-1,\ 1]$ using a Tanh nonlinear activation function, ensuring that the classical features can be accurately mapped to the rotation angle of the quantum state.

4.4. VQC-Based Quantum Classifier

To process classical information within a quantum system, the output vectors must first be converted into physical parameters of quantum states. Here, the features are linearly scaled to the $[-\pi, \pi]$ radian space, such that each classical dimension corresponds to the rotation angle of a single qubit. Through angle encoding, the classical data are

transformed into the initial states of the VQC. Inspired by data re-uploading [35], RY-gate-based encoding structures are embedded into each variational layer to further enhance the classification expressiveness of the VQC. This design repeatedly injects classical information into deeper circuit layers, effectively strengthening the model's ability to characterize complex nonlinear decision boundaries.

After data encoding, deep feature correlations are learned through the VQC. The model constructs 4 variational layers, each composed of a strongly entangling architecture formed by learnable rotation gates and CNOT gates. Through entanglement operations between neighboring qubits, the circuit establishes long-range correlations among features in a high-dimensional Hilbert space. An evolution space composed of multiple qubits is employed, and the rotation-gate parameters in each layer are optimized via backpropagation to achieve optimal feature representation.

The final outcome of the quantum evolution must be converted back into classical values to enable the final class decision. At the end of the circuit, expectation-value measurements of the Pauli-Z operator are performed on all qubits. The measurement projects the complex quantum state onto eight real-valued outputs within the range $[-1, 1]$, forming a classical output vector. This vector aggregates features enhanced by quantum interference and entanglement and is subsequently used as the input to the post-quantum processing layer. This layer effectively aggregates the information captured in the quantum states, projects it onto classification logits, and then feeds these logits into a Softmax function to determine the predicted probability distribution over attack types.

5. Results and Discussion

5.1. Experimental Settings

The experimental datasets are generated through sampling based on the CVQKD physical model described in Figure 1. The dataset comprises 5 classes: under no attack, LOIA, calibration attacks, saturation attacks, and hybrid attacks. For each physical scenario, $N = 10^7$ valid pulses are independently sampled. The raw sequences are then truncated into pulse blocks with a size of Q = 10,000, where each block serves as an individual sample. Consequently, each category contains 1000 samples, resulting in a total dataset of 5000 pulse blocks. Finally, the dataset is partitioned into training and testing sets with a ratio of 4:1.

The model optimization employs the categorical cross-entropy loss function, with the Adam optimizer selected for global parameter updates. The learning rates are tailored according to the distinct gradient sensitivities of the classical and quantum modules within the hybrid architecture. Specifically, the learning rate for the classical convolutional layers is set to 10^{-4} to ensure the stable extraction of spatial statistical features. Conversely, the learning rate for the quantum variational layers is set to 10^{-3}. Since variational circuits possess fewer parameters and exhibit higher sensitivity to gradient fluctuations, a larger learning rate facilitates a rapid search for the optimal representation within the Hilbert space.

5.2. Evaluation Metrics

To validate the classification efficacy of our proposed HQCNN in processing CVQKD attack data, we employ the confusion matrix as the basis for analysis. Let TP, TN, FP, and FN denote true positives, true negatives, false positives, and false negatives, respectively. The specific evaluation metrics are defined as follows:

- Accuracy: The proportion of correctly classified samples relative to the total population, reflecting the model's overall discriminative capability across the dataset.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}. \tag{13}$$

- Precision: Also known as positive predictive value, it represents the fraction of actual positive instances among the samples predicted as a specific category. In the context of attack detection, higher precision indicates a lower false alarm rate.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}. \tag{14}$$

- Recall: Also known as sensitivity, it signifies the proportion of actual instances of a category that are correctly identified by the model.

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}. \tag{15}$$

- F1-score: The harmonic mean of precision and recall, providing a balanced assessment that accounts for both false negatives (missed detections) and false positives (false alarms).

$$\text{F1} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}. \tag{16}$$

5.3. Experimental Analysis of Qubit Scaling

To determine the optimal number of qubits for the proposed HQCNN, we constructed and compared models with qubit counts $n \in \{4, 6, 8, 10\}$. According to the training accuracy curves in Figure 3, the following observations can be made: All models exhibit a rapid upward trend within the first 20 epochs. Throughout the entire 100-epoch training process, the 8-qubit HQCNN demonstrates the most robust and superior performance, characterized by relatively minor fluctuations and a final accuracy closest to 1.0. Notably, even in lower-dimensional Hilbert spaces with 4 or 6 qubits, the models still achieve recognition accuracies exceeding 90%. This performance is attributed to the data re-uploading mechanism implemented across the 4 variational layers. By re-injecting feature information into each layer, this mechanism enhances the capability of individual qubits to characterize nonlinear boundaries.

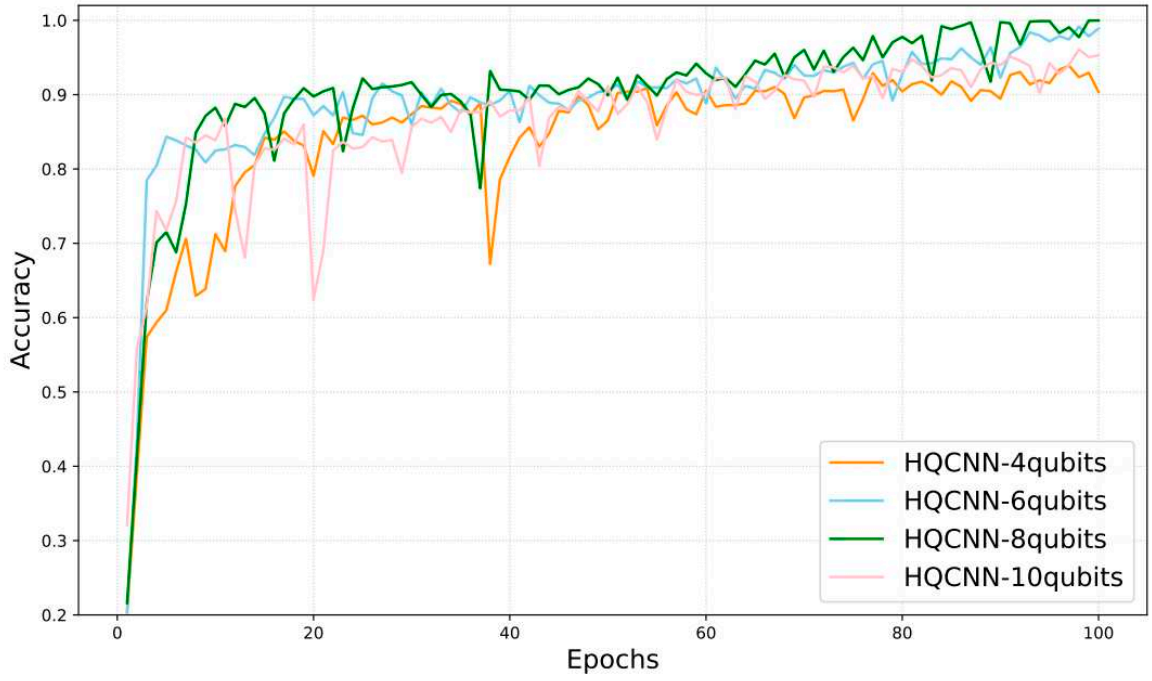

Figure 3. Comparison of training accuracy for HQCNN models with 4, 6, 8, and 10 qubits.

However, when the number of qubits increases to 10, the model performance does not continue to improve with the additional quantum resources. As shown in Figure 3, the accuracy curve of the 10-qubit model remains comparable to that of the 6-qubit configuration and does not surpass the performance of the 8-qubit model. It is important to note that the 10-qubit model does not exhibit severe training instability, as its accuracy still converges to a level above 90%. Instead, the results suggest that further increasing the Hilbert space dimension does not necessarily lead to better classification performance for the current dataset.

The expressive capacity of the VQC grows rapidly with the number of qubits due to the strongly entangling layers. When the model capacity becomes significantly larger than the intrinsic complexity of the dataset, the optimization process may become less efficient, resulting in marginal performance gains. In this case, the 8-qubit configuration appears to provide a more suitable balance between model expressivity and training stability. Therefore, the experimental results indicate that 8 qubits represent an effective operating point for the proposed HQCNN architecture, achieving the best trade-off between representational power and optimization efficiency.

5.4. Evaluation and Analysis of Model Performance

To evaluate the performance enhancement of the hybrid quantum-classical architecture in CVQKD attack detection, we select the ResNet [36] as the baseline for comparison. By maintaining consistency in feature extraction depth between the convolutional layers of the HQCNN and the residual modules of ResNet, this experiment effectively isolates the impact of the VQC versus classical fully connected layers when processing highly overlapping physical features.

Furthermore, considering the potential overfitting tendency of ResNet on datasets of a specific scale, a "Best Model Saving" mechanism was specifically implemented. At the end of each training epoch, a synchronous validation is performed on the test set. By real-time monitoring of the test accuracy, the mechanism preserves only the set of model weights that achieves the historical peak performance. This strategy ensures that the models utilized for final performance analysis remain in their optimal generalization state throughout the training cycle, thereby effectively eliminating the interference of overfitting on the experimental comparisons.

The experimental results of the hybrid quantum–classical architecture and ResNet are summarized in Table 1, and the corresponding confusion matrices are presented in Figure 4. For each attack class, Table 1 reports the recall, F1-score, and accuracy. In addition, the overall accuracy represents the overall classification accuracy across all samples and is defined as

$$Acc_{overall} = \frac{N_{correct}}{N_{total}}, \tag{17}$$

where $N_{correct}$ denotes the number of correctly classified samples and N_{total} is the total number of test samples. The results indicate that the overall recognition accuracy of HQCNN is 6% higher than that of ResNet. Regarding category-specific metrics, both models achieve a precision and recall of 1.00 for the calibration, saturation, and hybrid attacks, where physical features are highly distinct.

The HQCNN achieves a recall of 0.90 for LOIA, whereas ResNet only reaches 0.66, implying that ResNet would face a higher risk of missed detections in practical deployments. Analysis of the confusion matrices reveals that ResNet suffers from severe bidirectional confusion between the normal state and LOIA. In contrast, while the HQCNN still misclassifies some normal samples as LOIA, it exhibits a more decisive identification capability for the LOIA attack.

Table 1. Performance comparison between HQCNN and ResNet across different scenarios: under no attack (NA), LOIA (LA), calibration attacks (CA), saturation attacks (SA), and hybrid attacks (HA).

Class	Model	Recall	F1-Score	Accuracy	Overall Accuracy	
					HQCNN	ResNet
NA	HQCNN	0.88	0.72	0.80	0.93	0.87
	ResNet	0.66	0.66	0.66		
LA	HQCNN	0.76	0.90	0.83		
	ResNet	0.66	0.66	0.66		
CA	HQCNN	1.00	1.00	1.00		
	ResNet	1.00	1.00	1.00		
SA	HQCNN	1.00	1.00	1.00		
	ResNet	1.00	1.00	1.00		
HA	HQCNN	1.00	1.00	1.00		
	ResNet	1.00	1.00	1.00		

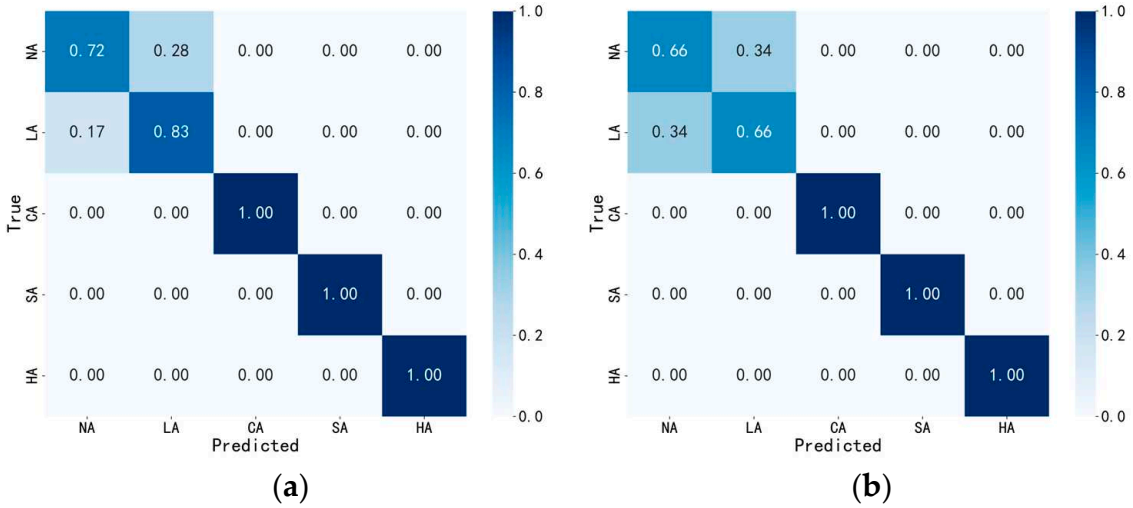

Figure 4. Normalized confusion matrices for (**a**) the HQCNN and (**b**) ResNet.

From a physical perspective, the difficulty in distinguishing LOIA from the no-attack state originates from the statistical properties of quadrature measurements in GMCS-CVQKD. Under normal operation, Bob's measured quadrature values follow an approximately Gaussian distribution with variance σ^2. In a LOIA scenario, Eve manipulates the local oscillator intensity by introducing a scaling factor $k < 1$, which effectively rescales the shot-noise unit and slightly modifies the variance of the measured quadratures. Importantly, this attack does not significantly alter the overall distribution shape, which remains approximately Gaussian with zero mean. Consequently, the statistical difference between the two states is mainly reflected in subtle variance changes rather than obvious structural patterns, making them difficult to distinguish for conventional classifiers.

The proposed HQCNN is better suited to capture such subtle statistical differences. After the classical CNN extracts statistical features from pulse sequences, the angle encoding mechanism maps these features into rotation angles of qubits. Small changes in the variance of the quadrature measurements lead to corresponding variations in the quantum rotation angles, which modify the interference patterns of the quantum states in the Hilbert space. Through the Strongly Entangling Layers, correlations among multiple statistical features can be jointly represented, enabling the model to amplify subtle distribution differences that may remain indistinguishable in classical Euclidean feature space. As a result,

the HQCNN exhibits improved sensitivity to LOIA compared with the purely classical ResNet architecture.

5.5. Parameter Complexity Analysis

To estimate the parameter requirements of a classical network that provides a comparable transformation capacity, consider a classical fully connected layer mapping an input feature vector of dimension d to a feature space of dimension 2^n. The number of trainable parameters required is

$$N_{FC} = d \times 2^n + 2^n. \tag{18}$$

In our model, the classical feature extractor outputs a feature vector of dimension $d = 32$. Therefore, implementing a comparable linear mapping would require $N_{FC} = 32 \times 256 + 256 = 8448$ parameters for a single layer. However, a single linear layer cannot capture the high-order feature interactions that arise naturally in quantum entanglement operations. To approximate similar nonlinear correlations, a classical network typically requires multiple hidden layers. For example, a compact multilayer perceptron with architecture $32 \to 128 \to 128 \to 5$ would require approximately $(32 \times 128) + (128 \times 128) + (128 \times 5) \approx 21,000$ trainable parameters.

Similarly, if a lightweight CNN is used to model global feature correlations, multiple convolutional blocks and dense layers are required, typically leading to tens of thousands of parameters, even under compact design constraints.

In contrast, the core classification logic of the proposed HQCNN is executed by a VQC consisting of only 96 parameters. Despite its minimal parameter count, the VQC performs nonlinear transformations within a $2^8 = 256$-dimensional Hilbert space, enabling the mapping of low-dimensional, linearly inseparable attack features into high-dimensional, linearly separable decision states. This demonstrates the exceptional parameter efficiency of VQC when processing high-dimensional features.

This high efficiency stems from two fundamental physical properties of quantum computing. First, while classical bit states are linear, n qubits can exist in a superposition of 2^n states. Second, the StronglyEntanglingLayers allow for the correlation of global features with minimal parameters. In a classical ResNet, establishing similar long-range dependencies typically necessitates the stacking of multiple deep convolutional kernels. Therefore, leveraging a HQCNN for the detection of quantum hacking attacks in CVQKD achieves an optimal balance between model compactness and discriminative capability.

5.6. Security Analysis

The proposed HQCNN framework primarily serves as an auxiliary monitoring and attack detection mechanism for identifying potential quantum hacking attacks in CVQKD systems. In practical deployment, the quantum component of the HQCNN is intended to operate in a near-real-time manner to continuously monitor the system's operational status. Furthermore, since the quantum inference stage processes only compressed classical feature representations and does not require additional measurements or operations on the original optical signals in the quantum communication channel, the detection process can be carried out without affecting the real-time communication of the system.

In this scheme, data are compressed by classical layers before entering the quantum stage. This isolation design facilitates the protection of the original system's security. Specifically, the Pauli-Z measurements at the end of the VQC act only on the qubits. Physically, this design avoids any interference from the detection process on the original coherent states of the CVQKD system, ensuring that the HQCNN is non-intrusive to the system.

Furthermore, if an adversary attempts to infer sensitive internal information by eavesdropping on the VQC's output, they would find it virtually impossible to reverse-engineer the original signal distribution or key generation parameters. This is due to the preceding classical nonlinear mappings (e.g., ReLU, Tanh) and the significant dimensionality truncation, which collectively minimize the risk of side-channel leakage.

The hybrid model also remains resilient to adversarial attacks, where subtle input perturbations are used to compromise classification. To deceive the quantum decision-making process, an attacker must identify specific adversarial noise that can simultaneously bypass the classical CNN and the bottleneck layer mapping. These constraints, spanning both classical and quantum mathematical spaces, substantially increase the computational cost of finding effective adversarial examples, thereby ensuring the robustness of the detection model in complex adversarial environments.

6. Conclusions

This work addresses practical security defense challenges in CVQKD systems by designing and implementing a HQCNN architecture for identifying multiple quantum hacking attacks. The architecture employs classical CNN layers to extract and reduce key statistical features from signals, followed by VQC for efficient recognition and decision-making of complex attack patterns. Comparative experiments demonstrate that the overall accuracy of HQCNN surpasses that of the classical ResNet model by approximately 6%. Even with a significantly smaller number of parameters than ResNet, HQCNN still exhibits superior classification performance, achieving a dual improvement in model compactness and detection accuracy. This study not only provides a highly discriminative attack detection scheme for CVQKD systems but also, more importantly, offers technical support for future defenses over long-distance complex channels and the construction of large-scale quantum-secure networks through its demonstrated high parameter efficiency.

Author Contributions: Conceptualization, X.H.; Methodology, X.H.; Software, X.H.; Validation, X.H. and X.L.; Formal analysis, X.H.; Investigation, X.H.; Resources, J.X. and X.L.; Writing—original draft, X.H.; Writing—review & editing, J.X.; Visualization, X.H.; Supervision, J.X.; Project administration, J.X. All authors have read and agreed to the published version of the manuscript.

Funding: This study received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The datasets presented in this article are not readily available because the data are part of an ongoing study.

Acknowledgments: The authors would like to thank the anonymous reviewers for their valuable comments and suggestions that helped improve this manuscript.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

CVQKD	Continuous-variable quantum key distribution
HQCNN	Hybrid quantum-classical neural network
CNN	Convolutional neural network
VQC	Variational quantum circuit
LOIA	Local oscillator intensity attacks
ResNet	Residual network

QKD	Quantum key distribution
DVQKD	Discrete-variable quantum key distribution
GMCS	Gaussian modulated coherent state
ML	Machine learning
ANN	Artificial neural network
SVM	Support vector machine
QML	Quantum machine learning
DL	Deep learning
DNN	Deep neural network
QNN	Quantum neural network
NISQ	Noisy intermediate-scale quantum
MCTS	Monte Carlo tree search
AM	Amplitude modulator
PM	Phase modulator
PC	Polarization controller
CNOT	Controlled-NOT

References

1. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum Cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195. [CrossRef]
2. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian Quantum Information. *Rev. Mod. Phys.* **2012**, *84*, 621–669. [CrossRef]
3. Bennett, C.H.; Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
4. Ekert, A.K. Quantum Cryptography Based on Bell's Theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef]
5. Bennett, C.H. Quantum Cryptography Using Any Two Nonorthogonal States. *Phys. Rev. Lett.* **1992**, *68*, 3121–3124. [CrossRef]
6. Grosshans, F.; Grangier, P. Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef]
7. Leverrier, A.; Grangier, P. Continuous-Variable Quantum-Key-Distribution Protocols with a Non-Gaussian Modulation. *Phys. Rev. A* **2011**, *83*, 042312. [CrossRef]
8. Leverrier, A.; Grangier, P. Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation. *Phys. Rev. Lett.* **2009**, *102*, 180504. [CrossRef]
9. Ma, X.-C.; Sun, S.-H.; Jiang, M.-S.; Liang, L.-M. Local Oscillator Fluctuation Opens a Loophole for Eve in Practical Continuous-Variable Quantum-Key-Distribution Systems. *Phys. Rev. A* **2013**, *88*, 022339. [CrossRef]
10. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E. Preventing Calibration Attacks on the Local Oscillator in Continuous-Variable Quantum Key Distribution. *Phys. Rev. A* **2013**, *87*, 062313. [CrossRef]
11. Qin, H.; Kumar, R.; Alléaume, R. Quantum Hacking: Saturation Attack on Practical Continuous-Variable Quantum Key Distribution. *Phys. Rev. A* **2016**, *94*, 012325. [CrossRef]
12. Namiki, R.; Hirano, T. Security of Continuous-Variable Quantum Cryptography Using Coherent States: Decline of Postselection Advantage. *Phys. Rev. A* **2005**, *72*, 024301. [CrossRef]
13. Lodewyck, J.; Debuisschert, T.; García-Patrón, R.; Tualle-Brouri, R.; Cerf, N.J.; Grangier, P. Experimental Implementation of Non-Gaussian Attacks on a Continuous-Variable Quantum-Key-Distribution System. *Phys. Rev. Lett.* **2007**, *98*, 030503. [CrossRef] [PubMed]
14. Qin, H.; Kumar, R.; Makarov, V.; Alléaume, R. Homodyne-Detector-Blinding Attack in Continuous-Variable Quantum Key Distribution. *Phys. Rev. A* **2018**, *98*, 012312. [CrossRef]
15. Mao, Y.; Huang, W.; Zhong, H.; Wang, Y.; Qin, H.; Guo, Y.; Huang, D. Detecting Quantum Attacks: A Machine Learning Based Defense Strategy for Practical Continuous-Variable Quantum Key Distribution. *New J. Phys.* **2020**, *22*, 083073. [CrossRef]
16. Ding, C.; Wang, S.; Wang, Y.; Wu, Z.; Sun, J.; Mao, Y. Machine-Learning-Based Detection for Quantum Hacking Attacks on Continuous-Variable Quantum-Key-Distribution Systems. *Phys. Rev. A* **2023**, *107*, 062422. [CrossRef]
17. Du, H.; Huang, D. Multi-Attack Detection: General Defense Strategy Based on Neural Networks for CV-QKD. *Photonics* **2022**, *9*, 177. [CrossRef]
18. Schuld, M.; Sinayskiy, I.; Petruccione, F. An Introduction to Quantum Machine Learning. *Contemp. Phys.* **2015**, *56*, 172–185. [CrossRef]
19. Ciliberto, C.; Herbster, M.; Ialongo, A.D.; Pontil, M.; Rocchetto, A.; Severini, S.; Wossnig, L. Quantum Machine Learning: A Classical Perspective. *Proc. A* **2018**, *474*, 20170551. [CrossRef]

20. Sim, S.; Johnson, P.D.; Aspuru-Guzik, A. Expressibility and Entangling Capability of Parameterized Quantum Circuits for Hybrid Quantum-Classical Algorithms. *Adv. Quantum Technol.* **2019**, *2*, 1900070. [CrossRef]
21. Leyton-Ortega, V.; Perdomo-Ortiz, A.; Perdomo, O. Robust Implementation of Generative Modeling with Parametrized Quantum Circuits. *Quantum Mach. Intell.* **2021**, *3*, 17. [CrossRef]
22. Ma, X.-C.; Sun, S.-H.; Jiang, M.-S.; Gui, M.; Zhou, Y.-L.; Liang, L.-M. Enhancement of the Security of a Practical Continuous-Variable Quantum-Key-Distribution System by Manipulating the Intensity of the Local Oscillator. *Phys. Rev. A* **2014**, *89*, 032310. [CrossRef]
23. Iqbal, M.; Moreolo, M.S.; Muñoz, R.; Nadal, L. Machine Learning-Driven Attack and Fault Classification in CV-QKD Systems after Anomaly Detection. In Proceedings of the 2025 International Conference on Optical Network Design and Modeling (ONDM), Pisa, Italy, 6–9 May 2025; pp. 1–3.
24. Li, J.; Mao, Y.; Liao, Q.; Ding, Y.; Tang, Z.; Li, K. Detecting Quantum Hacking Attacks for Continuous-Variable Quantum Key Distribution Using Quantum Neural Network. *Chaos Solitons Fractals* **2026**, *202*, 117467. [CrossRef]
25. Li, S.; Cui, J.; Ren, J. Hybrid Classical–Quantum Neural Networks Enhanced by Quantum Architecture Search for Coronary Artery Stenosis Detection. *Neurocomputing* **2025**, *618*, 129111. [CrossRef]
26. Xia, R.; Kais, S. Hybrid Quantum-Classical Neural Network for Calculating Ground State Energies of Molecules. *Entropy* **2020**, *22*, 828. [CrossRef] [PubMed]
27. Liu, J.; Lim, K.H.; Wood, K.L.; Huang, W.; Guo, C.; Huang, H.-L. Hybrid Quantum-Classical Convolutional Neural Networks. *Sci. China Phys. Mech. Astron.* **2021**, *64*, 290311. [CrossRef]
28. Kabir, M.; Kaosar, M.; Laga, H.; Sohel, F. LHQNN: Sequential and Non-Sequential Layered Hybrid Quantum Neural Networks for Image Classification. *Quantum Mach. Intell.* **2025**, *7*, 51. [CrossRef]
29. Long, C.; Huang, M.; Ye, X.; Futamura, Y.; Sakurai, T. Hybrid Quantum-Classical-Quantum Convolutional Neural Networks. *Sci. Rep.* **2025**, *15*, 31780. [CrossRef]
30. Fan, F.; Shi, Y.; Guggemos, T.; Zhu, X.X. Hybrid Quantum-Classical Convolutional Neural Network Model for Image Classification. *IEEE Trans. Neural Netw. Learn. Syst.* **2024**, *35*, 18145–18159. [CrossRef]
31. Bokhan, D.; Mastiukova, A.S.; Boev, A.S.; Trubnikov, D.N.; Fedorov, A.K. Multiclass Classification Using Quantum Convolutional Neural Networks with Hybrid Quantum-Classical Learning. *Front. Phys.* **2022**, *10*, 1069985. [CrossRef]
32. Weedbrook, C.; Pirandola, S.; Ralph, T.C. Continuous-Variable Quantum Key Distribution Using Thermal States. *Phys. Rev. A* **2012**, *86*, 022318. [CrossRef]
33. Navascués, M.; Grosshans, F.; Acín, A. Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography. *Phys. Rev. Lett.* **2006**, *97*, 190502. [CrossRef] [PubMed]
34. García-Patrón, R.; Cerf, N.J. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503. [CrossRef] [PubMed]
35. Pérez-Salinas, A.; Cervera-Lierta, A.; Gil-Fuster, E.; Latorre, J.I. Data Re-Uploading for a Universal Quantum Classifier. *Quantum* **2020**, *4*, 226. [CrossRef]
36. He, K.; Zhang, X.; Ren, S.; Sun, J. Deep Residual Learning for Image Recognition. In Proceedings of the 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, 27–30 June 2016; pp. 770–778.