

CHSH Constrained Variational Attacks on the E91 Quantum Key Distribution Protocol

Tharso D. Fernandes, Demerson N. Gonçalves, Filippo Ghiglieri and Fernando M. Araújo-Moreira

Abstract— We investigate Quantum Circuit Learning (QCL) as a variational framework for exploring eavesdropping attacks on the entanglement-based E91 quantum key distribution protocol. Eve’s attack is modeled by a hardware-efficient parameterized quantum circuit optimized with a loss function combining the Clauser–Horne–Shimony–Holt (CHSH) parameter, the Alice–Bob quantum bit error rate (QBER), and Eve’s conditional bit-inference probability. We consider two attack models: a two-sided attack, in which Eve has coherent access to both distributed qubits before their delivery to Alice and Bob, and a one-sided attack restricted to an Alice–Eve interaction. In the noiseless two-sided scenario, the optimized circuit reaches $P_{\text{Eve}} \approx 0.79$, $S \approx 2.57$, and QBER $\approx 4.6\%$, while the corresponding CHSH-based lower bound on the asymptotic secret-key rate remains positive. Under depolarizing noise with probability $p = 0.1$, the two-sided attack remains inside the exploratory region $|S| > 2$ and QBER $< 8\%$, but the resulting key-rate lower bound becomes non-positive. In contrast, the one-sided attack reaches unit conditional inference probability only by causing a substantial QBER and eliminating Bell violation. These results show that variational circuits can explore information, disturbance regimes beyond fixed attack models, while the quantitative CHSH-based key-rate bound, rather than a binary Bell-violation or QBER threshold, is required to assess whether positive asymptotic secret-key extraction is certified.

I. INTRODUCTION

Quantum Key Distribution (QKD) is one of the most mature applications of quantum information science to secure communication systems. Its central promise is to establish secret keys whose security is grounded in physical principles rather than in computational assumptions. Since the seminal BB84 protocol [1] and the entanglement-based E91 protocol [2], QKD has become a fundamental building block for quantum communication networks, including fiber-based links, free-space optical channels, satellite-assisted architectures, and future quantum internet infrastructures [3], [4].

Practical QKD systems are subject to channel and device imperfections, so security must be assessed under realistic

noise models [5], [6].

Artificial intelligence and machine learning have recently emerged as useful tools for quantum communication systems. Learning-based methods have been investigated for protocol optimization, noise mitigation, error correction, parameter estimation, resource allocation, anomaly detection, and security enhancement in quantum networks [7], [8]. These developments suggest that learning algorithms can be used not only to improve the performance and reliability of quantum communication systems, but also to probe their vulnerabilities by optimizing adversarial strategies. This dual role is particularly relevant for QKD, where security is operationally characterized by the tradeoff between Eve’s information gain and the disturbance observed by Alice and Bob.

Quantum Circuit Learning (QCL) [11] has recently been applied to eavesdropping attacks on BB84 [12], recovering known individual attacks in the noiseless regime and discovering modified strategies in noisy channels. This suggests that trainable quantum circuits can serve as variational models for exploring information-disturbance tradeoffs in QKD. In parallel, a recent study by Dhakal *et al.* [13] presented a comprehensive performance analysis of BB84, E91, and an enhanced BB84 protocol under several noise models, including depolarizing and amplitude damping. Their work evaluated CHSH degradation and QBER using Qiskit simulations and highlighted that E91 preserves strong entanglement-based security under ideal conditions while becoming more sensitive under realistic noise. However, that analysis considered only a fixed intercept–resend eavesdropping model.

In this work we use QCL to investigate variational eavesdropping strategies against the E91 protocol under noiseless and depolarizing channels. Eve’s interaction with the distributed entangled pair is represented by a parameterized quantum circuit and optimized through a loss function that combines three security-relevant quantities: the Clauser–Horne–Shimony–Holt (CHSH) parameter S , the Alice–Bob quantum bit error rate (QBER), and Eve’s conditional success probability. Here, S is used both as a Bell–nonlocality indicator and as an input to the quantitative security analysis. Values with $|S| > 2$ witness nonlocal correlations, but the binary condition $|S| > 2$ alone does not certify a positive secret-key rate. The quantitative value of S , together with the QBER, determines the information bound used in the key-rate analysis. The formal definition of S and the CHSH test is given in the next section.

We compare two attack models with different operational meanings. The first is a two-sided attack, in which Eve acts jointly on Alice’s qubit, Bob’s qubit, and her ancilla

Tharso Dominisini Fernandes, Department of Pure and applied Mathematics, UFES, Alegre, ES, Brazil, e-mail: tharso.fernandes@ufes.br; Demerson N. Gonçalves, Department of Mathematics, CEFET-RJ, Petrópolis, RJ, Brazil, e-mail: demerson.goncalves@cefet-rj.br; Filippo Ghiglieri, Institute of Physics, University of Brasília, Brasília, DF, Brazil, e-mail: filippo.ghiglieri@df.ufscar.br; Fernando Manuel Araújo Moreira, Military Institute of Engineering (IME), Rio de Janeiro, RJ, Brazil, e-mail: fernando.manuel@ime.eb.br. All authors are also affiliated with the Military Institute of Engineering (IME), Rio de Janeiro, RJ, Brazil. This work was partially supported by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) and the Brazilian Ministry of Defense (through the PRÓ-DEFESA V Program – IATQ Network, grant No. 88887.961681/2024-00), as well as the Financiadora de Estudos e Projetos (FINEP) (through the projects PDI-DQBRN/1545-22, CMLabIME/0160-22, and QUANTUM II/3310-24.

through a three-qubit hardware-efficient ansatz (HEA). In the literature, a HEA is typically understood as a shallow variational circuit built from native single-qubit rotations and a simple entangling pattern, chosen to balance expressivity, trainability, and hardware compatibility [14]. The second is a one-sided attack restricted to an Alice–Eve interaction and implemented by a shallow two-qubit variational circuit with only four trainable parameters. This distinction separates a more expressive adversarial model, capable of perturbing both subsystems of the shared pair, from a restricted local model that accesses only one side of the entangled resource.

Our main contribution is to show that these two variational attack models lead to qualitatively different information–disturbance regimes in E91. In particular, the two-sided attack can achieve a substantial conditional bit-inference probability while remaining inside an exploratory low-disturbance region characterized by $|S| > 2$ and moderate QBER. The corresponding CHSH-based key-rate lower bound is then used to determine whether positive asymptotic secret-key extraction is certified. By contrast, the one-sided attack reaches very high inference probability only at the cost of strongly degrading the correlations and eliminating Bell violation. Thus, the contribution of this paper is not merely to transfer QCL from BB84 to E91, but to show that variationally learned attacks can reveal security-relevant operating points in entanglement-based QKD that are not captured by fixed attack models.

The remainder of this paper is organized as follows. Section II reviews the E91 protocol, including the singlet state, the CHSH test, the parameter S , and the role of raw-key generation and QBER. Section III presents the QCL framework, introduces the two-sided and one-sided attack models, and defines the composite loss function used in the optimization. Section IV reports and discusses the simulation results for noiseless and depolarizing channels. Finally, Section V concludes the paper and outlines directions for future work.

II. THE E91 PROTOCOL

A. Singlet State and CHSH Test

The E91 protocol is an entanglement-based quantum key distribution protocol whose security is certified through the violation of a Bell inequality. In its ideal form, Alice and Bob share pairs of qubits prepared in the singlet state

$$|\psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \quad (1)$$

Each party randomly chooses one of two possible measurement settings, corresponding to different orientations of their polarization analyzers. Alice uses angles $\{0, \frac{\pi}{2}\}$ and Bob uses $\{\frac{\pi}{4}, \frac{3\pi}{4}\}$, a standard choice for maximal CHSH violation with the singlet state. For the singlet state, this choice of relative orientations leads to a maximal Bell-inequality violation, up to the sign convention adopted for the correlation function.

The correlations between Alice’s and Bob’s binary outcomes are quantified by the CHSH parameter. Assigning measurement outcomes the values $a, b \in \{+1, -1\}$, the correlation function associated with the settings A_i and B_j is

$$E(A_i, B_j) = \sum_{a,b=\pm 1} ab P(a, b|A_i, B_j), \quad (2)$$

where $P(a, b|A_i, B_j)$ is the joint probability of obtaining outcomes a and b for the corresponding measurement settings. The CHSH parameter is then defined as

$$S = E(A_0, B_0) - E(A_0, B_1) + E(A_1, B_0) + E(A_1, B_1). \quad (3)$$

Classically, local hidden-variable theories satisfy $|S| \leq 2$, whereas quantum correlations can reach the Tsirelson bound $|S| = 2\sqrt{2}$.

Any local hidden-variable model satisfies the CHSH bound

$$|S| \leq 2, \quad (4)$$

whereas quantum mechanics allows violations up to the Tsirelson bound

$$|S| \leq 2\sqrt{2}. \quad (5)$$

For the ideal singlet state and the measurement angles given above, one obtains

$$S = -2\sqrt{2} \approx -2.828. \quad (6)$$

Thus, an observed violation $|S| > 2$ provides an operational witness of nonclassical correlations between Alice and Bob. Conversely, if $|S| \leq 2$, the observed correlations are compatible with a local classical description, and the key cannot be certified by the CHSH test alone. In this work, the CHSH parameter is used as the main detectability constraint: Eve’s attack is optimized to keep S as close as possible to $-2\sqrt{2}$, so that the legitimate users do not perceive a clear signature of eavesdropping.

B. Raw Key Generation

In the E91 protocol, part of the measurement data is used to estimate the CHSH parameter, while another part is used to generate the raw key. For the singlet state, when Alice and Bob use compatible key-generation settings, their outcomes are perfectly anti-correlated in the ideal noiseless case. After basis sifting and public discussion of the measurement settings, one party flips its bits so that Alice and Bob obtain identical raw keys.

In practical and noisy implementations, this anti-correlation is no longer perfect. Therefore, the quality of the raw key must be assessed together with the observed Bell violation. In the present QCL-based attack model, this role is played by the QBER, while the CHSH value S quantifies whether the correlations still exhibit nonclassical behavior. The security-relevant tradeoff studied in this work is therefore determined by the simultaneous behavior of S , QBER, and Eve’s success probability P_{Eve} .

III. QUANTUM CIRCUIT LEARNING FOR E91 ATTACKS

The attack models considered in this section are represented by Eve’s variational interaction blocks inserted after the source distributes the entangled pair and before Alice and Bob perform their local measurements.

A. Two-Sided Attack

In the two-sided attack model, Eve is assumed to control the source or the distribution stage. She prepares or coherently processes the joint state before delivering one qubit to Alice and one qubit to Bob, while retaining an ancillary system initialized in $|0\rangle$. She applies a three-qubit variational unitary $U(\theta)$ to the joint system formed by Alice's qubit, Bob's qubit, and her ancilla.

This corresponds to an untrusted-source threat model. It does not require Eve to access both qubits after they have been securely delivered to Alice and Bob; rather, it models coherent control of the distributed state before delivery. The two-sided model is therefore more expressive than the one-sided model and is used here as an adversarial upper model.

Figure 1 summarizes the protocol flow in this model. After Eve's interaction, the qubits are delivered to Alice and Bob, who choose their measurement settings and perform the measurements used to evaluate the CHSH parameter, the QBER, and Eve's success probability.

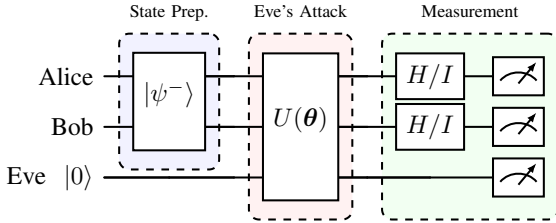


Fig. 1: Protocol flow for the two-sided attack.

The variational block $U(\theta)$ is implemented by a three-qubit hardware-efficient ansatz. Figure 2 shows one representative layer. In each layer, Alice's qubit, Bob's qubit, and Eve's ancilla undergo local R_X and R_Z rotations, followed by a ring of CNOT gates. Repeating this layer three times gives the full 18-parameter attack ansatz used in the simulations.

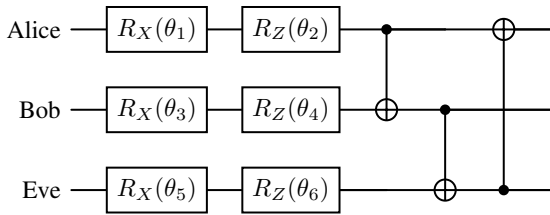


Fig. 2: One layer of $U(\theta)$.

Because Eve acts jointly on both subsystems of the shared pair and on her ancilla, this model captures a genuinely two-sided interaction. When noise is present, it is applied only to the Alice–Bob channel before Eve's variational operation.

B. One-Sided Attack

In the one-sided attack model, the source prepares a singlet pair and distributes one qubit to Alice and one to Bob, as in the standard E91 protocol. Eve then couples an ancilla to Alice's qubit and applies a two-qubit variational unitary

$V(\phi)$, with $\phi \in \mathbb{R}^4$, before Alice and Bob perform their local measurements.

Figure 3 shows the circuit used to represent $V(\phi)$. The two wires correspond to Alice's qubit and Eve's ancilla, so the interaction is restricted to one side of the distributed entangled pair, while Bob's qubit evolves without direct access from Eve. After this interaction, Alice and Bob perform the measurements used to evaluate the CHSH parameter, the QBER, and Eve's success probability.

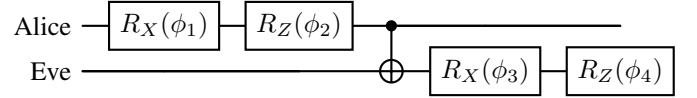


Fig. 3: Variational circuit representing the operator $V(\phi)$ for the one-sided attack, coupling only Alice's qubit and Eve's ancilla.

The circuit is intentionally shallow. Alice's qubit first applies local R_X and R_Z rotations, followed by a CNOT from Alice to Eve, and then Eve's ancilla applies R_X and R_Z rotations. This gives a total of four trainable parameters. Because Eve interacts only with Alice's subsystem, this model captures a one-sided attack. When noise is present, it is applied to the Alice–Bob channel before Eve's variational operation.

C. Loss Function and Security Metrics

The optimization of Eve's variational circuit is driven by three security-relevant quantities: the CHSH parameter S defined in Section II, the quantum bit error rate (QBER), and Eve's conditional success probability P_{Eve} . All three are evaluated directly from the output of the PennyLane circuits described above.

Quantum bit error rate. For the singlet state, Alice and Bob are ideally anti-correlated in the two key-generation bases. Therefore, when the QBER is evaluated from the raw measurement outcomes before Bob's bit flip, an error event corresponds to coincidence. We define the QBER as

$$\text{QBER} = \frac{1}{2} \sum_{\theta \in \{0, \pi/2\}} [P(0_\theta, 0_\theta) + P(1_\theta, 1_\theta)], \quad (7)$$

where $P(i_\theta, j_\theta)$ denotes the joint probability that Alice obtains i and Bob obtains j when both measure in the basis rotated by angle θ .

Eve's conditional success probability. The relevant quantity for the eavesdropper is the probability that she correctly guesses Alice's bit given that the pair contributes to the sifted key, i.e., given that Alice and Bob disagree in the raw outcomes. Using the three-qubit probability distribution $p(i, j, k)$ for Alice (i), Bob (j), and Eve (k), evaluated in one of the key-generation bases, we define

$$P_{\text{Eve}} = \frac{p(0, 1, 0) + p(1, 0, 1)}{p(0, 1, \cdot) + p(1, 0, \cdot)}, \quad (8)$$

where the denominator is the probability that the pair is kept for key generation.

The quantity P_{Eve} is evaluated for the specific measurement and decision rule implemented by Eve in the variational circuit. It is therefore an operational attack-performance metric and should not be identified directly with Eve's Holevo information. The latter is bounded independently from the observed CHSH value in the key-rate analysis.

Loss function. These three quantities are combined into the composite loss

$$\begin{aligned} \mathcal{L}(\theta) = & \alpha_S (S - S_{\text{target}})^2 \\ & + \alpha_{\text{QBER}} (\text{QBER} - \text{QBER}_{\text{target}})^2 \\ & - \alpha_P P_{\text{Eve}}. \end{aligned} \quad (9)$$

The first two terms penalize deviations from the target values $S_{\text{target}} = -2\sqrt{2}$ and $\text{QBER}_{\text{target}} = 0.1$, respectively, so that Eve aims to preserve correlations that appear normal to Alice and Bob. The last term, with negative sign, rewards Eve for maximizing her bit-inference probability. The coefficients $\alpha_S = \alpha_{\text{QBER}} = \alpha_P = 2$ are chosen empirically to produce balanced gradients during training.

In our optimization, we set $\text{QBER}_{\text{target}} = 0.10$. This value is used only as an exploratory optimization target, rather than as a formal E91 security threshold. It constrains the variational search to an empirically motivated moderate-disturbance regime, consistent with the low-percentage QBER values reported in entanglement-based QKD implementations [17], [18]. The formal security assessment is instead based on the CHSH-based key-rate lower bound r_{LB} . Therefore, deviations from this target constrain the optimization search but do not constitute a security criterion.

The loss is minimized with the Adam optimizer, using learning rate 0.1 for 200 steps. All expectation values and probabilities are computed on the `default.mixed` device, so that noise channels are properly accounted for.

D. Secret Key Rate Analysis

To assess whether the optimized attacks are compatible with positive secret-key extraction, we use a CHSH-based bound on the asymptotic Devetak–Winter secret-key rate [15], [19]. For the considered collective attack model, the relevant rate is written as

$$r_{\text{LB}}(S, Q) = 1 - h_2(Q) - I_E^{\text{ub}}(S), \quad (10)$$

where $Q = \text{QBER}$, $h_2(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ is the binary entropy, and $I_E^{\text{ub}}(S)$ is an upper bound on Eve's Holevo information.

For $2 \leq |S| \leq 2\sqrt{2}$, we use

$$I_E^{\text{ub}}(S) = h_2\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2}\right). \quad (11)$$

For $|S| < 2$, the observed CHSH correlations do not provide a nontrivial CHSH-based device-independent bound on Eve's information. In this case, we use the trivial bound

$$I_E^{\text{ub}}(S) = 1, \quad |S| < 2, \quad (12)$$

which yields

$$r_{\text{LB}} = -h_2(Q). \quad (13)$$

A positive value of r_{LB} certifies a positive asymptotic secret-key rate under the adopted assumptions. Conversely, a non-positive value does not by itself prove that the protocol is insecure; it indicates that a positive key rate is not certified by the adopted bound.

The reported quantity is an asymptotic lower bound under the collective-attack model and the assumptions associated with the CHSH-based information bound. Finite-size effects, detector imperfections, channel losses, parameter-estimation penalties, and error-correction inefficiency are not included in the present analysis.

IV. RESULTS AND DISCUSSION

Table I summarizes the final values of S , QBER, and P_{Eve} after optimization. The corresponding learning curves are shown in Fig. 4.

Scenario	S	P_{Eve}	QBER	r_{LB}
Two-Sided noiseless	-2.5688	0.7887	0.0459	0.2719
Two-Sided depol. ($p = 0.1$)	-2.3775	0.6837	0.0797	-0.0782
One-Sided noiseless	-1.4142	1.0000	0.2500	-0.8113
One-Sided depol. ($p = 0.1$)	-1.0622	1.0000	0.3122	-0.8957

Positive r_{LB} certifies a positive asymptotic secret-key rate under the adopted assumptions.

TABELA I: Final metrics after optimization. The quantity r_{LB} is the conservative lower bound on the asymptotic secret-key rate obtained from the CHSH-based upper bound on Eve's information.

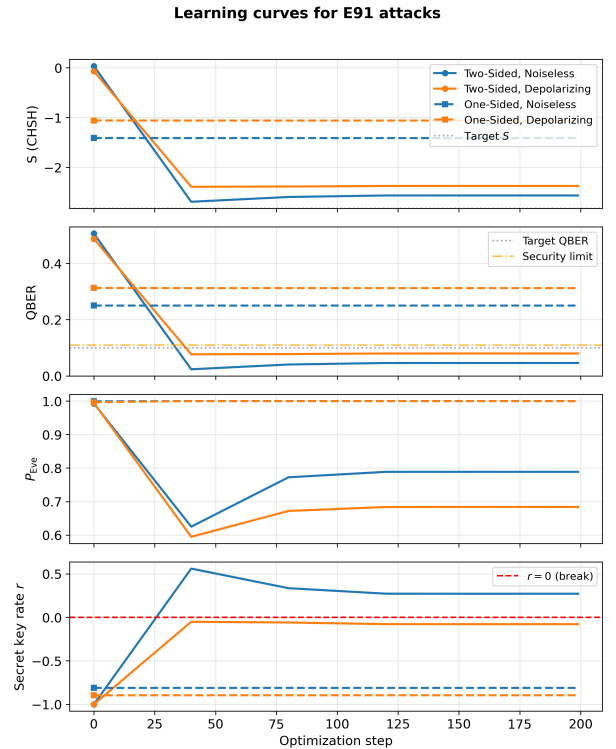


Fig. 4: Learning curves for the optimized attacks. Solid lines: two-sided; dashed lines: one-sided.

The results reveal a sharp contrast between the two attack models. In the noiseless setting, the two-sided attack converges

to a regime in which the Bell violation remains strong, with $|S| \approx 2.57$, while the QBER stays at only 4.6%. At the same time, Eve reaches a conditional success probability of about 79%. Crucially, the CHSH-based lower bound on the asymptotic secret-key rate remains positive, $r_{LB} \approx 0.272$. Thus, under the adopted assumptions, the optimized leakage is compatible with positive secret-key extraction. The attack does not establish a break of E91 in this noiseless operating point, because the estimated information leakage can still be handled by the corresponding information-theoretic security bound.

Under depolarizing noise, the two-sided attack still achieves $P_{Eve} \approx 0.68$ while keeping $|S| > 2$ and QBER below 8%, but the CHSH-based lower bound becomes non-positive, $r_{LB} \approx -0.078$. This does not by itself prove that the protocol is insecure; it indicates that a positive asymptotic secret-key rate is not certified by the adopted bound in this regime. This transition is not captured by the simple threshold checks on S and QBER alone, which would still place this operating point inside the exploratory acceptance region defined by the CHSH and QBER thresholds. Thus, the secret key rate provides a more reliable security diagnostic.

By contrast, the one-sided attack reaches $P_{Eve} = 1$ in both the noiseless and depolarizing cases, but only at the cost of severely degrading the correlations shared by Alice and Bob, resulting in non-positive values of the conservative key-rate bound, $r_{LB} \approx -0.81$ and -0.90 , respectively. Since $|S| < 2$ in these cases, the calculation uses the trivial bound $I_E^{ub} = 1$. Such a large disturbance would be immediately visible to the legitimate users.

V. CONCLUSION

In this work, we applied QCL to explore two classes of eavesdropping attacks on the entanglement-based E91 protocol. The attacks were trained with a loss function that simultaneously drives the CHSH parameter toward its ideal value, constrains the QBER to an exploratory moderate-disturbance regime, and maximizes Eve's conditional bit-inference probability. We complemented this exploratory threshold analysis with a CHSH-based lower bound on the asymptotic Devetak–Winter secret-key rate.

The simulations revealed qualitatively different information–disturbance regimes for the two attack models. In the noiseless case, the two-sided variational attack reached $P_{Eve} \approx 0.79$, while maintaining $|S| \approx 2.57$ and QBER $\approx 4.6\%$. The corresponding lower bound $r_{LB} \approx 0.272$ remained positive, so positive asymptotic secret-key extraction was certified under the adopted assumptions.

Under depolarizing noise with $p = 0.1$, the two-sided attack maintained $|S| > 2$ and QBER below 8%, but the lower bound became non-positive, $r_{LB} \approx -0.078$. This means that the adopted analysis no longer certifies a positive asymptotic secret-key rate in this regime. The result illustrates why a binary Bell-violation test or an exploratory QBER threshold, considered alone, is insufficient to certify positive key extraction.

The one-sided attack reached unit conditional inference probability only by causing a substantial QBER and elimi-

nating Bell violation. These results show that QCL provides a flexible framework for exploring adversarial information–disturbance tradeoffs in entanglement-based QKD. The learned conditional leakage metric can identify operating points that deserve further security analysis, while the quantitative CHSH-based key-rate bound determines whether positive asymptotic key extraction is certified under the adopted assumptions.

CODE AVAILABILITY

The code used in this study is available from the corresponding author upon request.

REFERÊNCIAS

- [1] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proc. International Conference on Computers, Systems and Signal Processing*, 175 (IEEE, 1984).
- [2] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” *Phys. Rev. Lett.* **67**, 661 (1991).
- [3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shaari, M. Tomamichel, G. Vallone, P. Villoresi, and P. Wallden, “Advances in quantum cryptography,” *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.
- [4] I. Mahmud and A. Abdelhadi, “Artificial Intelligence in Quantum Communications: A Comprehensive Survey,” *IEEE Access*, vol. 13, pp. 121174–121205, 2025, doi: 10.1109/ACCESS.2025.3585799.
- [5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” *Reviews of Modern Physics*, vol. 81, no. 3, pp. 1301–1350, 2009.
- [6] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher, and others, “Quantum key distribution: A networking perspective,” *ACM Computing Surveys*, vol. 53, no. 5, pp. 1–41, 2020.
- [7] M. Krenn, J. Landgraf, T. Foesel, and F. Marquardt, “Artificial intelligence and machine learning for quantum technologies,” *Physical Review A*, vol. 107, no. 1, p. 010101, 2023.
- [8] M. Mafu, “Advances in artificial intelligence and machine learning for quantum communication applications,” *IET Quantum Communication*, 2024.
- [9] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, “Quantum machine learning,” *Nature*, vol. 549, pp. 195–202, 2017.
- [10] M. Cerezo, A. Arrasmith, R. Babbush, S. C. Benjamin, S. Endo, K. Fujii, J. R. McClean, K. Mitarai, X. Yuan, L. Cincio, and P. J. Coles, “Variational quantum algorithms,” *Nature Reviews Physics*, vol. 3, pp. 625–644, 2021.
- [11] K. Mitarai, M. Negoro, M. Kitagawa, and K. Fujii, “Quantum circuit learning,” *Phys. Rev. A* **98**, 032309 (2018).
- [12] T. Decker, M. Gallezot, S. F. Kerstan, A. Paesano, A. Ginter, and W. Wormsbecher, “Quantum key distribution as a quantum machine learning task,” *arXiv:2508.12345* (2025).
- [13] P. Dhakal, B. R. Dawadi, and N. B. Adhikari, “Performance analysis of different quantum key distribution protocols for optimised security and efficiency,” *IET Quantum Communication*, vol. 6, no. 1, pp. e70015, 2025.
- [14] A. Kandala, A. Mezzacapo, K. Temme, M. Takita, M. Brink, J. M. Chow, and J. M. Gambetta, “Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets,” *Nature*, vol. 549, pp. 242–246, 2017, doi: 10.1038/nature23879.
- [15] 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. 98, no. 23, p. 230501, 2007.
- [16] V. Bergholm et al., “PennyLane: Automatic differentiation of hybrid quantum-classical computations,” *arXiv:1811.04968* (2018).
- [17] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, et al., “Entanglement-based quantum communication over 144 km,” *Nature Physics*, vol. 3, no. 7, pp. 481–486, 2007.
- [18] J. Yin, Y.-H. Li, S.-K. Liao, et al., “Entanglement-based secure quantum cryptography over 1,120 kilometres,” *Nature*, vol. 582, no. 7813, pp. 501–505, 2020.
- [19] I. Devetak and A. Winter, “Distillation of secret key and entanglement from quantum states,” *Proceedings: Mathematics, Physical and Engineering*, pp. 207–235, 2005.