# A Comparative Review Between Measurement-Device Independent QKD Protocols

**Mario C. Ribeiro**[*,1,2], **Alexandre B. Tacla**[1], **Fernando de Melo**[2], **and Raul O. Vallejos**[2]
[1]*QuIIN - Quantum Industrial Innovation, EMBRAPII CIMATEC Competence Center in Quantum Technologies, SENAI CIMATEC, Salvador, BA, Brazil*

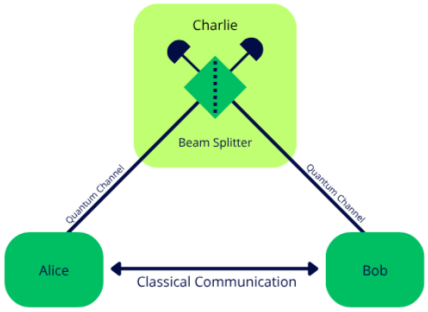
[2]*Centro Brasileiro de Pesquisas Físicas, Rio de Janeiro, Rio de Janeiro, Brazil*
[*]*Centro Brasileiro de Pesquisas Físicas; R. Dr. Xavier Sigaud, 150 - Botafogo, Rio de Janeiro - RJ; mcurvo@cbpf.br*

**Abstract: Measurement-device-independent quantum key distribution (MDI-QKD) marks an important step toward commercially viable quantum security by neutralizing all side-channel attacks against detection hardware. This review provides a comparative analysis between discrete-variable (DV) and continuous-variable (CV) MDI-QKD systems. Here, we give a general overview on some of the main protocols in the field, evaluating performance trade-offs by comparing secret key rates against distance under realistic channel conditions, as well as security proof techniques, finite-key limitations, and practical implementation complexity.**
**Keywords: Quantum Key Distribution. Measurement Device Independent. Quantum Cryptography**
**Abbreviations: QKD, Quantum Key Distribution. MDI, measurement device independent. CV, continuous variable. DV, discrete variable. TF, twin-field. QPSK, quadrature phase shift keying. BB84, Bennet-Brassard 1984. BSM, Bell-state measurement. BS, beam splitter. PBS, polarizing beam splitter.**

## 1. Introduction

In quantum key distribution (QKD), two parties, commonly called Alice and Bob, seek to establish a shared secret key over an insecure quantum channel, while preventing any information leakage to a potential eavesdropper, Eve. Among the many challenges in ensuring this security, detector-side-channel attacks are one of the main vulnerabilities in practical QKD implementations [1]. For example, in a discrete-variable (DV) QKD system, where single photon detection is critical, an eavesdropper might use bright light to "blind" the detectors, forcing them to operate in a classical regime. In this way, an attacker can obtain control of the detectors' output and gain knowledge on the key without being detected. This is called a "blinding attack", and is one of many different strategies that exploit detector-side imperfections [2]. In a general measurement-device independent quantum key distribution (MDI-QKD) protocol, two distant parties, Alice and Bob, independently prepare and transmit quantum states to an untrusted third party, or relay, named Charlie, as described in Figure 1. Charlie performs measurements on the incoming states and publicly broadcasts the results. Crucially, these outcomes only reveal corre-

**Figure** 1: Simple general schematic of a MDI-QKD protocol




Alice and Bob send quantum signals to a central relay (Charlie), who interferes them using a beam splitter and measures them; Alice and Bob then establish a secure key via classical communication based on the relay's measurement results.

lations between Alice's and Bob's data, not their private encoding choices. This measurement effectively projects their independent states into a maximally entangled Bell state, forming the basis of their shared secret key. Because of this, any type of detector side-channel attack is removed from the equation. The core principle of MDI-QKD is that even if Eve has complete control over Charlie's measurement apparatus, she cannot learn the key. Any attempt to tamper with the measurement will inevitably introduce statistical errors in the correlations, which Alice and Bob can detect during classical post-processing. The unique architecture of MDI-QKD fundamentally changes the roles of the communicating parties and the nature of the quantum measurement, being perfectly suited for star-shaped quantum networks (multiple users connecting to a central relay). In this work, we will discuss the main ideas of MDI-QKD protocols both in a discrete variable scenario, covering the original MDI-QKD [3] and its variant Twin-Field QKD [4, 5]. Then, we discuss the continuous variable (CV) framework, discussing the original MDI-CV-QKD with Gaussian modulation [6] as well as the QPSK modulation protocol [7]. Finally, we will make a comparative analysis between the advantages and downsides of each strategy.

## 2. Discrete-Variable MDI-QKD

### 2.1. The Original MDI-QKD Protocol

The protocol proposed by Lo, Curty and Qi (2012) [3] operates as follows:

1. **State Preparation:** Alice and Bob independently prepare weak coherent pulses, encoding random bits into one of four polarization states (e.g., horizontal, vertical, +45°, or -45°), and transmit these pulses to the central relay, Charlie.

2. **Bell-State Measurement (BSM):** At the relay, the pulses interfere on a 50:50 beam splitter. The outputs are then directed through polarizing beam splitters (PBS) to four single-photon detectors. Specific combinations of detector "clicks" herald a successful BSM outcome, which Charlie publicly announces.

3. **Sifting and Key Distillation:** Alice and Bob sift their data, keeping only the rounds where they used the same encoding basis (e.g., both used the rectilinear or both used the diagonal basis) and where Charlie reported a successful BSM. The BSM result creates a direct correlation between Alice's and Bob's bits. Following sifting, they perform parameter estimation, error correction, and privacy amplification to distill a final, secure key.

### 2.2. Security Proof

The security of MDI-QKD is elegantly proven by establishing its equivalence to a virtual, entanglement-based BB84 [8] protocol. One can imagine that instead of preparing and sending polarization states, Alice and Bob each begin with a qubit that is entangled with the photon they send. For instance,

$$|\psi\rangle_A = \frac{|H\rangle_A|H\rangle_a + |V\rangle_A|V\rangle_a}{\sqrt{2}} \tag{1}$$

where mode A refers to the "virtual" qubit and mode $a$ denotes the polarized photon sent to the relay. Bob prepares his state analogously. Alice and Bob measuring their local qubit in the $Z$ or $X$ basis is mathematically equivalent to randomly preparing the photon in the corresponding polarization state. Since this virtual measurement can be conceptually delayed until after Charlie's detection, a successful BSM at the relay effectively establishes an entangled Bell state between Alice's and Bob's virtual qubits, such as

$$|\psi\rangle_{AB} = \frac{|H\rangle_A|V\rangle_B \pm |V\rangle_A|H\rangle_B}{\sqrt{2}}. \tag{2}$$

This transforms the protocol into an entanglement-based BB84 scenario, where Eve is distributing entangled states, and the parties can independently measure their qubits in the $Z$ or $X$ basis, performing the protocol in the same fashion. This enables the MDI-QKD protocol to follow the same security proof of a BB84 protocol, resulting in a similar key rate expression. This expression is given by the Devetak-Winter rate [9]:

$$r_{DW} = I(A:B) - I(A:E), \tag{3}$$

where $I(A:B)$ is the mutual information between Alice and Bob and $I(A:E)$ is the mutual information between Alice and Eve. It can conveniently be rewritten in terms of the protocol error rates, rendering the expression:

$$r_{BB84} = 1 - h(E_X) - h(E_Z), \tag{4}$$

where $h[E_{X(Z)}]$ is the binary entropy of the X-basis (Z-basis) error rate. This security proof holds against collective attacks in the asymptotic limit (of rounds of the protocol) and can be extended to cover general coherent attacks via the quantum de Finetti theorem [10]. Under realistic parameters (*e.g.,* GHz source, 0.2 dB/km fiber loss), this protocol can achieve key rates of approximately 1 kbps at distances of the order of 100 km, with a maximum theoretical distance of around 230 km.

The security analysis in the asymptotic limit considers an idealized scenario with infinitely many rounds of the protocol. For pratical applications, however, one has to consider how to extend the security analysis to consider a finite number of rounds. A finite-key analysis has been made by Curty et al [11] in which they use large deviation theory in order to upper bound the finite-sized terms that appear in the secret key rate analysis. This is enough to guarantee security even in the case of general, coherent attacks. Thus, MDI-

QKD has its security and composability demonstrated in the finite scenario, rendering estimations of 100bps at 100km, while using $10^{14}$ number of rounds and the same settings previously mentioned.

### 2.3. Twin-Field QKD

The biggest MDI experiments using discrete variables in recent years have come in the form of a variant of the original MDI-QKD protocol, known as Twin-Field QKD [4][5]. In this scheme, Alice and Bob each prepare optical pulses in which the quantum state is either a single photon or the vacuum, with the logical information encoded in the relative phase of the prepared state. These pulses are sent to a central relay (Charlie), where the two incoming fields, one typically containing a single photon and the other being vacuum, are interfered on a beam splitter. Instead of performing a full Bell-state measurement, Charlie registers a single-photon detection event. Such an event reveals a correlation in the encoded phases of Alice's and Bob's states, which they can use, after classical communication and postprocessing, to distill a shared secret key. This seemingly simple change allows the secret key rate to scale with the square root of the channel transmittance $(\sqrt{\eta})$, rather than linearly $(\eta)$ as in previous protocols. This overcomes the fundamental rate-distance limit for repeaterless QKD (known as the Pirandola-Laurenza-Ottaviani-Banchi bound [12]), enabling communication over unprecedented distances. Experimentally, TF-QKD has achieved a secure key transmission over 1002 km of optical fiber [13], demonstrating its immense potential for building global-scale quantum networks.

## 3. Continuous-Variable MDI-QKD

### 3.1. Gaussian-Modulated CV-MDI-QKD

The MDI concept was extended to the continuous-variable framework by Pirandola et al [6], eliminating detector vulnerabilities for CV-QKD systems. In this protocol, Alice and Bob each prepare coherent states with quadrature components $x$ and $p$ which are realizations of two i.i.d. random variables $X$ and $P$ drawn from zero-centered continuous Gaussian distributions. These states are transmitted to Charlie, who performs a CV Bell detection. This involves interfering the two incoming fields at a 50:50 beam splitter and using two homodyne detectors to measure the quadratures of the output modes (*e.g.,* the $\hat{X}$ quadrature of one output and the $\hat{P}$ quadrature of the other). Charlie publicly broadcasts his real-valued measurement results. These outcomes establish a strong linear correlation between Alice's and Bob's Gaussian data, from which they can estimate channel parameters, perform information reconciliation, and distill a secure secret key through privacy amplification. A key advantage of this approach is its inherent compatibility with standard, off-the-shelf telecommunication hardware, although it is generally more sensitive to channel loss and excess noise than DV systems.

### 3.2. Security Proof

Similar to its DV counterpart in the asymptotic limit, the security of Gaussian-modulated CV-MDI-QKD is proven in an equivalent entanglement-based scheme where Alice and Bob start with a two-mode squeezed vacuum states (an EPR state). They perform heterodyne detection on their local modes, which projects the remote modes sent to Charlie into coherent states. Since this is indistinguishable to Eve from the prepare-and-measure version, its equivalence is assured. The key-rate expression also comes from the Devetak-Winter rate [9]:

$$r_{CV} = \beta I(A:B) - \chi(E:B), \tag{5}$$

where $\beta$ is the information reconciliation efficiency and Eve's information is given by the Holevo quantity $\chi(E:B)$ when considering reverse information reconciliation protocols. A critical result for CV-QKD is that for Gaussian modulation, the optimal attack Eve can perform is also Gaussian [14]. With a reconciliation efficiency of $\beta \approx 0.97$ and considering the most optimal setting with Alice closer to the relay (around 100m) and Bob at 20 km, the protocol can achieve key rates of the order of 10 mbps, significantly higher than its DV counterpart [6]. However, the maximum distance that the protocol is able to produce a secret key is much more limited, and the rate goes to zero at around 25 km. A composable security proof against general coherent attacks considering a finite number of rounds has been made by Ghorai et al [15]. There, they use a Gaussian version of the de Finetti Theorem to prove security against coherent attacks in the non-asymptotic case for different types of protocols that share certain symmetries, including the Gaussian modulated MDI-CV-QKD. More recently, Hajomer et al [16] showed achievable 2.6mbps secret key rates over a 10 km fiber link, considering collective attacks within the finite-size regime.

### 3.3. Discrete Modulation MDI-CV-QKD

In their 2019 work [7] the authors propose a long-distance CV-MDI-QKD protocol using discrete modulation. More specifically, they use a four-state Quadrature Phase-Shift Keying (QPSK) modulation scheme, which simplifies the experimental setup and post-processing, resulting in a more noise-tolerant key rate. Instead of Alice and Bob drawing random values from a continuous Gaussian distribution, they prepare and send one of four distinct coherent states, corresponding to the four points of the QPSK constellation. The untrusted relay, Charlie, performs the standard MDI-CV measurement. This approach offers several practical benefits. It simplifies state preparation and data processing, and it allows for the use of more efficient error-correcting codes that are well suited for discrete alphabets, especially at low signal-to-noise ratios. Although discrete-modulated protocols generally yield lower key rates than their Gaussian-modulated counterparts

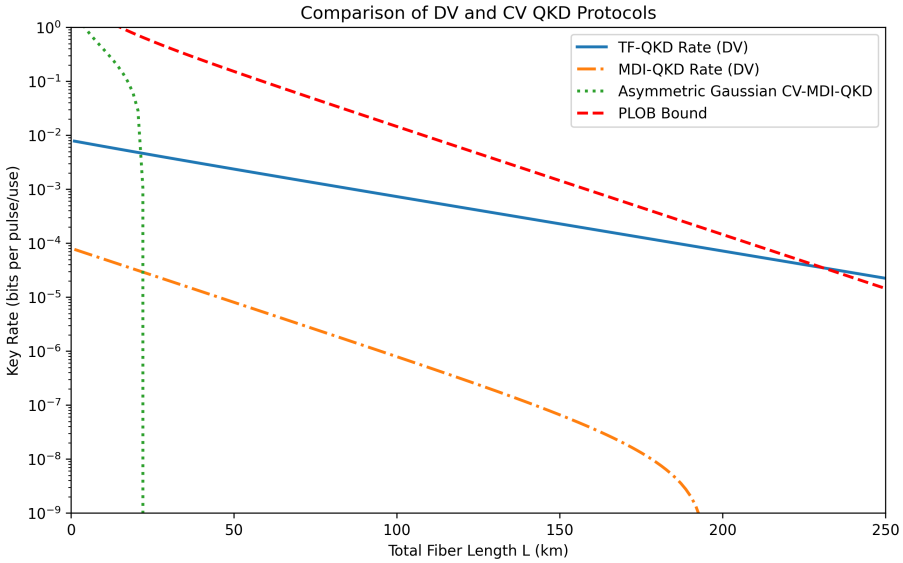
at short distances, they can exhibit greater robustness to excess noise, potentially extending the maximum achievable distance. For instance, theoretical analysis of a four-state protocol shows that it can generate a secure key at distances over 10 km farther than the equivalent Gaussian-modulated protocol under certain noisy conditions [7]. The security analysis is more complex due to the non-Gaussian nature of the states, often relying on numerical methods like semidefinite programming (SDP) to establish tight security bounds against collective attacks [17].

## 4. Comparative Discussion

The four MDI-QKD protocols reviewed (original MDI-QKD, Twin-Field QKD, Gaussian-modulated CV-MDI-QKD, and discrete-modulated CV-MDI-QKD) each occupy a distinct niche in the landscape of secure quantum communications. The primary trade-off governing protocol selection is the balance between the achievable secret key rate and the maximum transmission distance. As illustrated in Figure 2, which plots the secret key rate against distance, a clear performance hierarchy emerges. For high-rate metropolitan networks operating under 40 km, CV-MDI-QKD protocols are the undisputed leaders; Gaussian-modulated CV-MDI-QKD offers the highest potential key rates at the Mbps level, making it ideal for high-throughput applications. As distance increases over the functional range of CV protocols, DV-MDI-QKD protocols become an alternative, and when considering long-haul backbone networks exceeding 200 km, Twin-Field QKD is currently the only viable solution. By fundamentally altering the scaling of key rate with distance, it has shattered previous distance records and made continental-scale QKD a possibility, though this extreme range comes at the cost of very low key rates at its maximum reach.

Beyond this rate-versus-distance trade-off, practical implementation considerations are important. CV-QKD protocols generally use standard, room-temperature telecommunications components, making them significantly more cost-effective and easier to integrate with existing fiber optic infrastructure. In contrast, high-performance DV protocols can rely on sophisticated and expensive technology, such as superconducting nanowire single-photon detectors (SNSPDs) that require cryogenic cooling, posing possible a barrier to widespread deployment. The field of MDI-QKD has matured to a point where different protocols are optimized for distinct, complementary roles within a future quantum internet. The most promising path forward likely involves creating hybrid quantum networks. In such an architecture, high-rate CV-MDI-QKD systems would serve metropolitan and access networks, while TF-QKD would form the long-haul backbone connecting cities across the globe. Future research will continue to push the boundaries of performance. For CV-QKD, efforts are focused on

**Figure** 2: Comparative graph of secret key rate per relay use vs. total fiber length between different MDI QKD protocols.




In red, the PLOB bound [12], in blue, the CAL-19 [5] Twin-Field QKD protocol, in yellow, the original MDI-QKD [3] protocol and in green, the Gaussian-modulation CV-MDI-QKD [6] in its asymmetric version. The discrete-variable protocols both assume symmetric channel losses and parameters (signal intensity $\mu_s = 0.02$, dark count $Y_{00} = 10^{-8}$, detector error $e_d = 0.01$ and basis probabilities $p_{XX} = p_{ZZ} = 0.5$). The continuous variable protocol is modeled asymmetrically with a fixed Alice-to-relay distance of 1km, with Bob's distance varying, and excess noise 0.01. Key rates are calculated using the analytical expressions provided in the original papers, parameterized by the channel transmittance $\eta = 10^{-\gamma L/10}$ where the fiber attenuation coefficient is set to $\gamma = 0.2$ dB/km.

developing more efficient information reconciliation algorithms to improve key rates and extend the secure distance. For DV-QKD, work is ongoing to enhance source and detector technologies to further boost performance. For all protocols, developing more accessible and tighter finite-size security proofs remains a critical goal to ensure their security in practical applications.

## Acknowlegement

This work has been fully funded by the project "Receptores não-convencionais em CV-QKD" supported by QuIIN - Quantum Industrial Innovation, EMBRAPII CIMATEC Competence Center in Quantum Technologies, with financial resources from the PPI IoT/Manufatura 4.0 of the MCTI grant number 053/2023, signed with EMBRAPII.

## References

[1] Y. Zhao, F. C.-H. Fung, B. Qi, C. Chen, and H.-K. Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. Phys. Rev. A, 78:042333, 2008.

[2] Sebastien Sauge, Lars Lydersen, Andrey Anisimov, Johannes Skaar, and Vadim Makarov. Controlling an actively-quenched single photon detector with bright light. Opt. Express, 19(23):23590–23600, Nov 2011.

[3] H.-K. Lo, M. Curty, and B. Qi. Measurement-device-independent quantum key distribution. Phys. Rev. Lett., 108:130503, 2012.

[4] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature, 557:400–403, 2018.

[5] M. Curty, K. Azuma, and H.-K. Lo. Simple security proof of twin-field type quantum key distribution protocol. npj Quantum Information, 5(1):64, 2019.

[6] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen. High-rate measurement-device-independent quantum cryptography. Nature Photonics, 9:397–402, 2015.

[7] H.-X. Ma, P. Huang, D.-Y. Bai, T. Wang, S.-Y. Wang, W.-S. Bao, and G.-H. Zeng. Long-distance continuous-variable measurement-device-independent quantum key distribution with discrete modulation. Phys. Rev. A, 99:022322, 2019.

[8] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science, 560:7–11, 1984. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[9] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. Proc. Math. Phys. Eng. Sci., 461(2053):207–235, 2005.

[10] R. Renner. Security of quantum key distribution. International Journal of Quantum Information, 6(01):1–127, 2008.

[11] M. Curty, F. Xu, W. Cui, C. C. Wen, K. Tamaki, and H.-K. Lo. Finite-key analysis for measurement-device-independent quantum key distribution. Nature Communications, 5:3732, 2014.

[12] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi. Fundamental limits of repeaterless quantum communications. Nature Communications, 8:15043, 2017.

[13] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, and J.-M. Xiong. Experimental twin-field quantum key distribution over 1000 km fiber distance. Phys. Rev. Lett., 130:210801, 2023.

[14] Miguel Navascués, Frédéric Grosshans, and Antonio Acín. Optimality of gaussian attacks in continuous-variable quantum cryptography. Phys. Rev. Lett., 97:190502, Nov 2006.

[15] Shouvik Ghorai, Eleni Diamanti, and Anthony Leverrier. Composable security of two-way continuous-variable quantum key distribution without active symmetrization. Phys. Rev. A, 99:012311, Jan 2019.

[16] A. A. E. Hajomer, U. L. Andersen, and T. Gehring. High-rate continuous-variable measurement device-independent quantum key distribution with finite-size security. Quantum Science and Technology, 10:025032, 2025.

[17] Shouvik Ghorai, Philippe Grangier, Eleni Diamanti, and Anthony Leverrier. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. Phys. Rev. X, 9:021059, Jun 2019.