Bench Tests in Digital Signal Modulation as Preparation for CV-QKD Setup Creation

João Vitor Fraga de Carvalho Santos¹, Christiano Moreira de Sá do Nascimento¹, Valéria Loureiro da Silva¹
¹SENAI CIMATEC Technological Initiation – Competence Center in Quantum Technologies,
EMBRAPII; Salvador, Bahia, Brazil

Nowadays, quantum key distribution cryptography using continuous variables (CV-QKD) has emerged as a promising approach for the telecommunications industry, owing to its enhanced security and ease of integration with the coherent communication systems currently in use. In this context, this work presents the construction of a classical communication system for testing, with a future goal of transitioning to the quantum regime, focusing on the manipulation of equipment for signal modulation.
Keywords: Modulation. CV-QKD. Setup. Python.

Quantum key distribution (QKD) cryptography is a method of secret key transmission that enables secure communication between two authenticated parties, commonly referred to in the literature as Alice and Bob, without the risk of information being intercepted by an unauthenticated party [1].The great advantage presented by QKD protocols, in contrast to classical cryptography methods, is that their security is tied to the properties of quantum mechanics—such as Heisenberg's uncertainty principle and the no-cloning theorem—whereas classical methods like RSA rely on computational complexity; this implies that QKD protocols possess stronger security against technological advances such as quantum computing [1,2].

QKD communication protocols are divided into two types: discrete-variable QKD (DV), such as BB84, which utilizes single photons for information transmission, and continuous-variable QKD (CV), which employs light properties, including position and momentum, to encode information. A major advantage of CV-QKD is its similarity to commercially used coherent communication systems, which facilitates its implementation in current transmission networks [3,4].

Following the principles of coherent communication, it is possible to implement and use digital modulation methods—such as BPSK, QPSK, and QAM—to perform cryptography using CV-QKD [5,6].

This work aims to demonstrate the creation of a test bench for cryptographic systems using CV-QKD, focusing on the control of equipment used for the modulation of classical optical signals, ultimately preparing them for the assembly of a CV-QKD system.

Materials and Methods

Considering the focus of this work on the previously mentioned digital modulations, it is helpful to analyze their operation. The constellations are based on two sinusoidal signals, referred to as I (In-line) and Q (Quadrature), with a phase difference of $\pi/2$ between them, which are then combined to obtain the final signal. PSK (Phase-Shift Keying) modulations use phase shifts to represent symbols, with the shift value depending on the PSK type: BPSK (Binary PSK) manipulates only the I wave, with phase shifts of 0 and π *rad*; QPSK (Quadrature PSK), on the other hand, divides the key between the I and Q waves, applying respective phase shifts to obtain phases of 0, $\pi/2$, π, and $3\pi/2$ rad [5].Unlike PSK modulations, QAM constellations vary the amplitudes of the I and Q signals to encode each symbol, with normalized amplitudes in 16QAM ranging between 0.33 and 1 V [6].

Figure 1 illustrates the configuration of components adopted for the practical realization of these modulations, in which a laser was connected to an I/Q modulator via an optical fiber through a polarization controller. The arbitrary waveform generator (AWG) was connected to the I/Q modulator via an RF cable, and the bias voltage controller (BIAS CTRL) was connected via optical fibers with electrical feedback. Finally, the bias voltage controller used an optical fiber to connect to the photodetector, which in turn was connected to an oscilloscope.

For efficient control of the equipment, a Python code library was developed, primarily utilizing the PyVISA library to connect to instruments, model them, and communicate with them to control test parameters as desired [7].Each device had its own code model and complexity—for instance, the laser received commands for activation and deactivation, while the oscilloscope could automatically save the obtained results.

Among the instruments modeled by the library, the AWG stood out for its greater functional complexity compared to the others, such as codes for generating modulated waveforms. These functions were implemented to receive the secret key and generate a sinusoidal wave according to the requested modulation type, in a file format compatible with the AWG. Afterward, the library provided commands to send the signal to the AWG, select the desired output channel, activate that channel, and enable the equipment's operation.

The creation and use of the code library allowed precise and synchronized control of the equipment, establishing a functional system for testing. For each generated signal and obtained result, a low-pass filter was applied to reduce noise. These procedures were implemented to enhance the quality of the tests and improve the visualization and validation of the results.

Results and Discussion

As discussed, fine control of the instruments in the system produced concrete results. The data obtained by the oscilloscope were first processed, as previously mentioned, to generate graphical representations of their quadratures, allowing for the retrieval of the original key. The results are illustrated in the following figures: the BPSK constellation is shown in Figure 2, the QPSK in Figure 3, and the 16QAM in Figure 4.

The results show that the symbol detection points are correctly positioned within the decision intervals, indicating no ambiguity or errors during signal generation, transmission, detection, or processing. The positioning of these points enabled the retrieval of the original symbol set and the reconstruction of the initial key, confirming the validity of the system built during the project. From these results, the feasibility of generating quantum signals for key transmission is validated through signal attenuation and the introduction of a local oscillator for phase recovery [8].

Conclusion

This work demonstrated the capability of the developed system to transmit information through modulated signals, thereby preparing it for the transition from a classical system to a quantum system using CV-QKD. An improvement in the

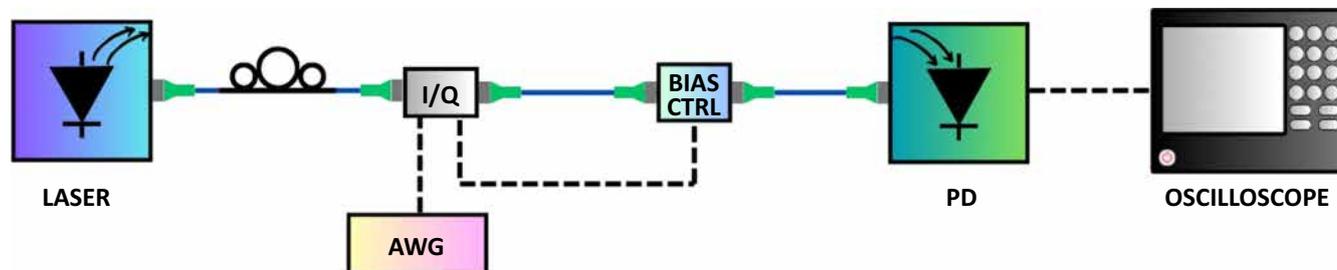**Figure 1.** Configuration of the signal generation, transmission, and reception system.

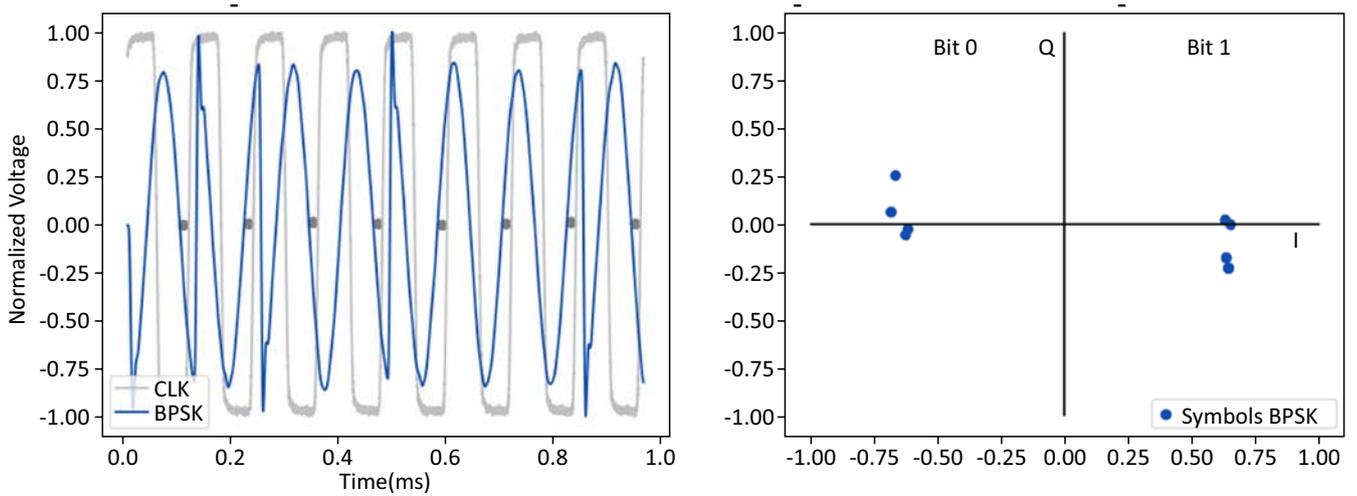**Figure 2.** BPSK signal and its constellation diagram.

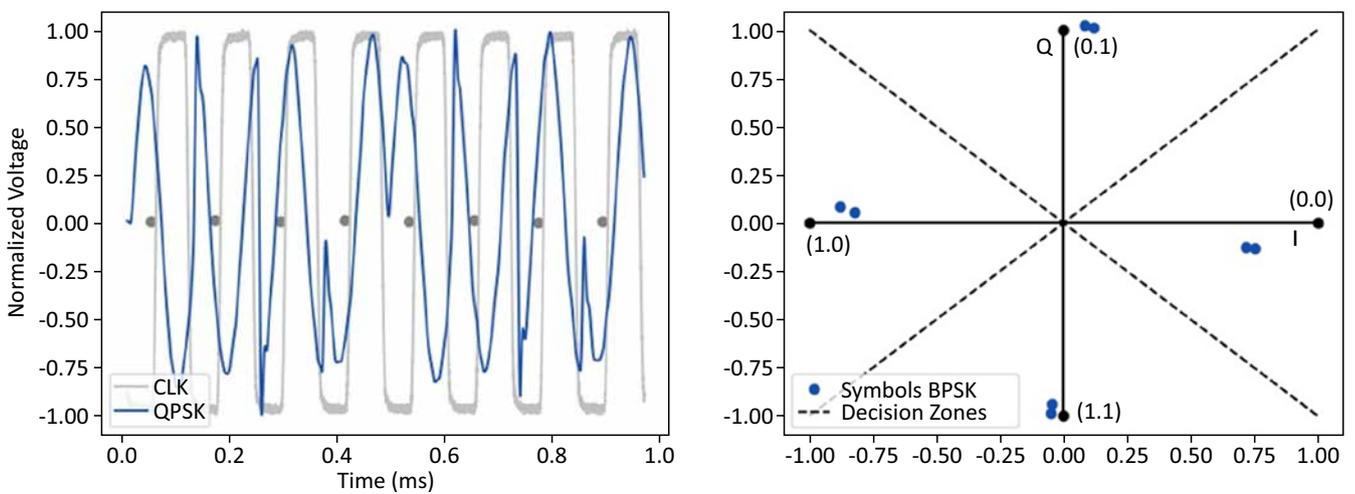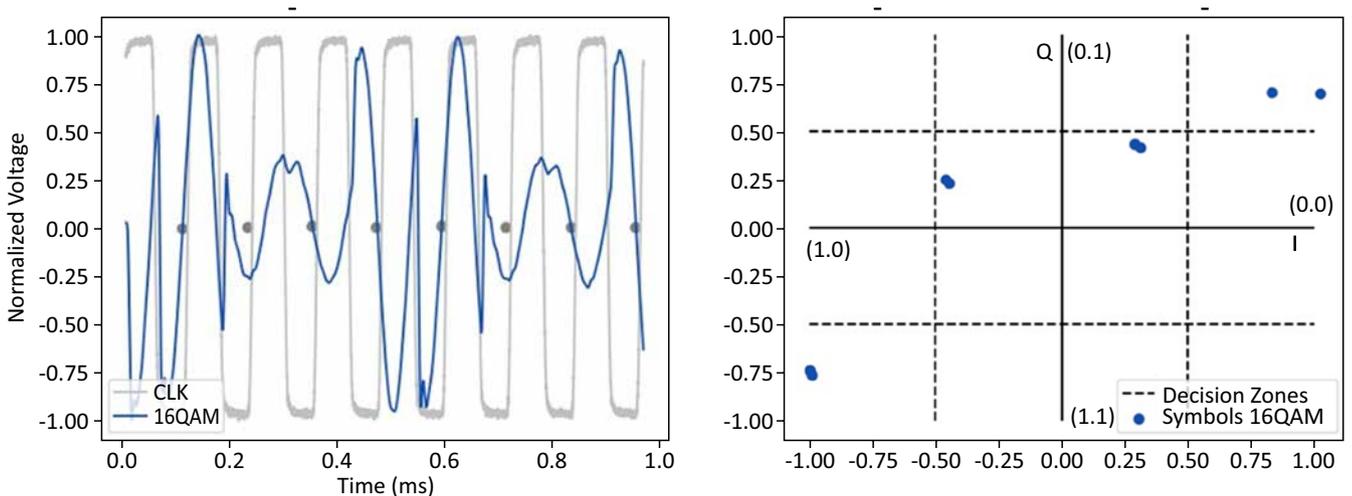**Figure 3.** QPSK signal and its constellation diagram.

Figure 4. 16QAM signal and its constellation diagram.

precision of the obtained constellation diagrams is also expected in the future, bringing them closer to the ideal decision-zone points as the transmission and modulation system is updated and optimized. Future steps for the project include transitioning from the classical to the quantum domain, testing additional modulation types—such as higher-order QAM constellations (e.g., 64QAM)—conducting free-space optical tests, and studying which variables most affect the constellation diagram.

Acknoledgments

References

1. Wolf R. Introduction. In: Quantum Key Distribution: An Introduction With Exercises. Cham: Springer; 2021. p. 1-12. (Vol. 988).

2. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978 Feb 1;21(2):120-6.

3. Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. Theor Comput Sci. 2014 Dec 4;560(P1):7-11.

4. Zhang Y, et al. Continuous-variable quantum key distribution system: past, present, and future. Appl Phys Rev. 2024 Mar 1;11(1).

5. Neto VS. Sistemas de Comunicação – Serviços, Modulação e Meios de Transmissão. In: Érica, editor. Rio de Janeiro: [s.n.]; p. 71-4.

6. Alencar MS, Da Rocha VC. Communication Systems. Cham: Springer International Publishing; 2022.

7. PyVISA: Control your instruments with Python. Disponível em: https://pyvisa.readthedocs.io/en/latest/.

8. Gisin N, et al. Quantum cryptography. Rev Mod Phys. 2001 Jan 19;74(1):145-95.