UNIVERSITY OF BELGRADE

PHOTONICA2025

Simulation and adaptation of DPS and DQPS QKD protocols for practical implementation and coexistence within PON architecture

Nemanja Miljkovic, Petar Matavulj
School of Electrical Engineering,University of Belgrade, Serbia
e-mail: mnemanja92.etf@gmail.com

INTRODUCTION

Technology of quantum computing and quantum computers is no longer topic of the future but the topic which represents one of the main focuses of nowadays research with fast traction and concrete practical results in last years. Taking this into account it became clear that all modern encryption algorithms will face serious challenges in incoming years especially if secure key exchange can't be guaranteed. One of considered approach to overcome this problem is technology of Quantum Key Distribution (QKD) that guarantees key exchange security by the laws of fundamental physics. Previous decades of research led to various practical implementations of QKD with constant pressure for further improvement of performances while lowering down costs of the placement of this new technology within existing optical network infrastructure. Result of this urge are new protocols and new methodologies with one goal to simplify and expand possibilities of integration within modern optical networks including Passive Optical Network (PON).

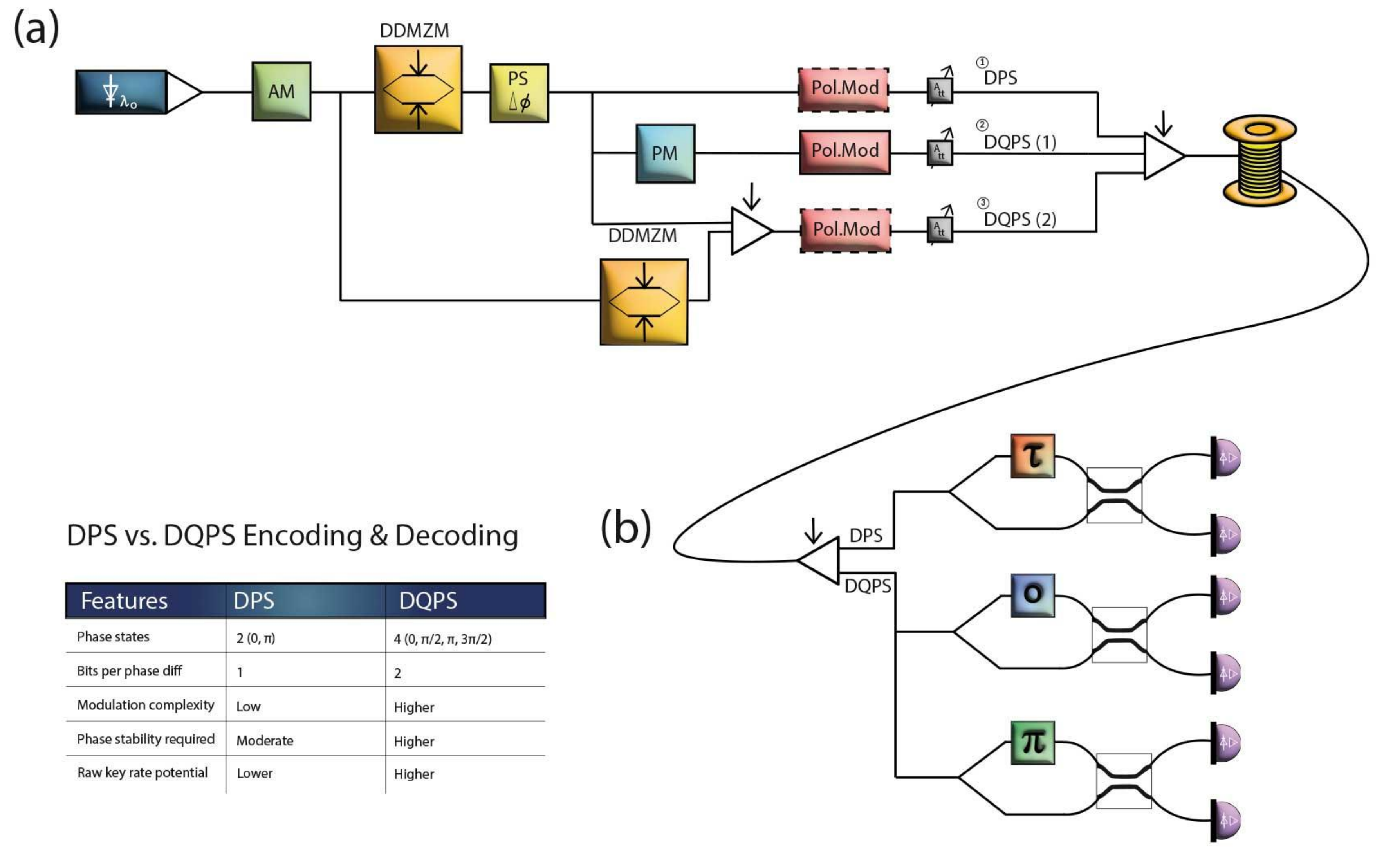
Due to the fact that implementing QKD within PON has some specific requirements, like simple and low-cost integration and multi-user scalability, there was a need for pairing it with newly developed protocols like Differential Phase Shift QKD (DPS QKD) and Differential Quadrature Phase Shift QKD (DQPS QKD) [1]. Results of recent studies, covering practical network implementation [2], also showed that these protocols are probably the best fit for first generation of Quantum Access Network (QAN).

In our previous work we were focused on most mature and most widely implemented QKD protocols BB84 and B92 where we proposed generalized QKD authentication architecture to enhance security of authentication mechanism [3]. We performed simulation and system characterization for this architecture with main focus on comparing performances of three proposed schemes.

MAIN CONCEPTS

In this paper our focus is on simulation, characterization and adaptation of DPS-QKD and DQPS-QKD aimed for integration and coexistence within PON architecture, with special focus on state-of-the-art versions of GPON and NG-PON2 [4]. Following principles from our previous research we are investigating which adaptations of mentioned protocols and their combination can result in most secure and yet most easy to implement solution for QKD integration within PON. General authentication architecture is proposed for this set of protocols and different variations of the setup are simulated and compared.

Initial scheme of transmitter, and its components, intended for DPS QKD protocol is presented over the top (1st) line of Fig. 1 (a). AM (Amplitude Modulator) is used for modulating laser signal power while using variations of input parameters of DDMZMs (Dual Drive Mach-Zehnder Modulator) and PS (Phase Shift) component we can perform phase modulation of the signal as required by DPS QKD protocol (0^o, 180^o). In order to gain more general model, that can be used for DQPS QKD protocol, we proposed two additional schemes (presented on 2nd and 3rd line of Fig. 1 (a). These schemes should modify DPS scheme's signal output so that final output signal has four different phase modulated signals used in DQPS protocol (0^o, 90^o , 180^o, 270^o).



DPS vs. DQPS Encoding & Decoding

Features	DPS	DQPS
Phase states	2 (0, π)	4 (0, π/2, π, 3π/2)
Bits per phase diff	1	2
Modulation complexity	Low	Higher
Phase stability required	Moderate	Higher
Raw key rate potential	Lower	Higher

Fig. 1: Optoelectronic scheme for authentication of DPS and DQPS QKD protocols.

Using set of optical switches in transceiver we are controlling which protocol and which scheme will be used on Alice side and this information is exchanged with Bob in order to configure optical switch on his side accordingly. Attenuators are used to attenuate signal further if needed and polarization modulators are placed as optional for further development of security of DPS and DQPS QKD protocols by adding polarization change as additional parameter. Representation of DPS and DQPS QKD receiver is given on Fig. 1 (b). As predicted by these protocol delay lines are used to make one bit delay in one of the branches after which it is compared weather phase difference exists between bit n and n+1. For DQPS we predicted additional phase delay, in the same time delay branch, in order to have additional parameter which can be used to improve security of the system as information about additional phase shift (if introduced) is shared over authenticated channel to Alice by Bob. Signals from both branches are then coupled and sent to single photon photodetectors.

KEY WORDS

DPS and DQPS QKD, QKD system modelling, QKD protocol simulation

SIMULATION RESULTS

After setting up previously explained concepts we perform simulations in order to confirm, compare and present obtained results. Simulation model was made, in OptiSystem toolkit, using schemes, shown in Fig. 1. All input parameters are chosen so that, previously explained concepts are maintained and satisfied. Following principles introduced in [3] for DV-QKD protocols, all parameters are previously calculated so that transition functions of every subsystem gives us proper output signal states for both DPS and DQPS QKD protocols. Simulations are performed with focus on signal power and phase characteristic at the output of transmitter and before photodetectors on receiver side in order to confirm that for defined parameters signal transmission is as predicted by protocols.

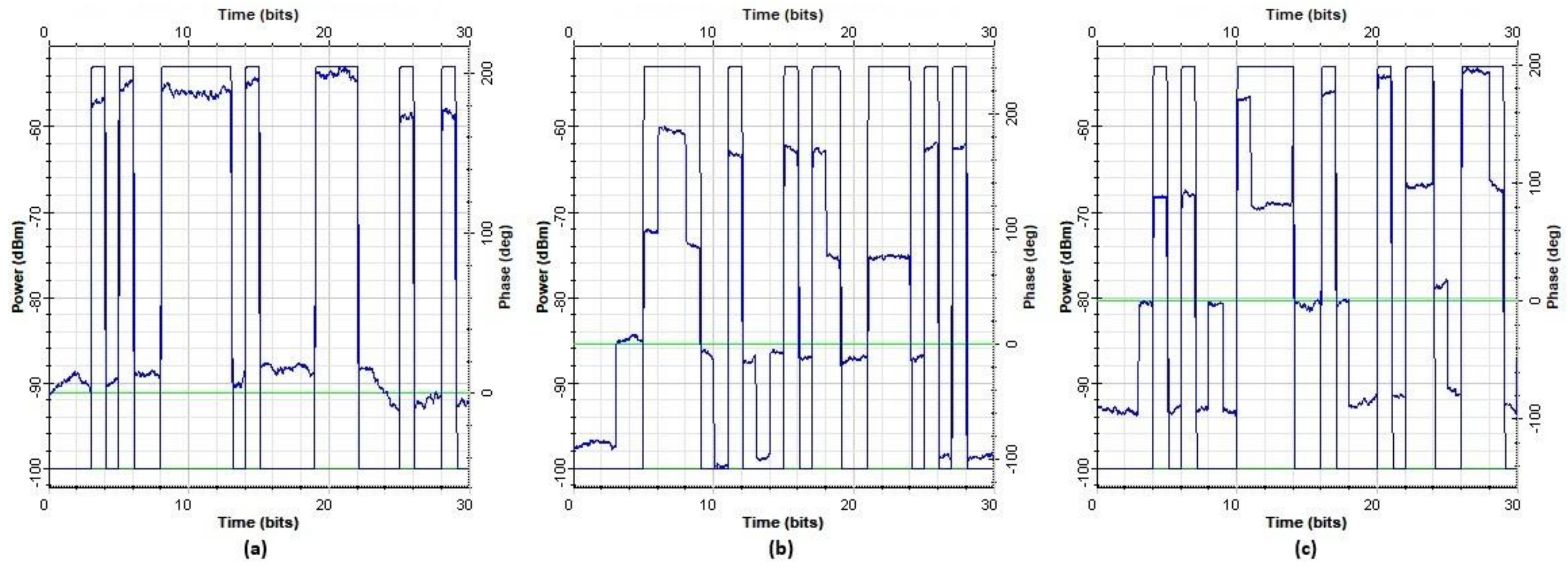


Fig. 2: Receiver output signal power and phase simulation results for DPS (a), DQPS (1) (b) and DQPS (2) (c) based on three different schemes presented in Fig 1. (a)

On Fig. 2 three graphs, (a), (b) and (c), represent output signal of transmitter for DPS, DQPS (1) and DQPS (2) schemes respectively, where simulation setup was based on transmitter architecture presented in Fig. 1 (a). Appropriate modulation is achieved by proper choice of input parameters for all components from the diagram. On Fig 3. there are graphs for receiver output signal power and phase for each receiver branch for both DPS (a), (b) and DQPS (d), (e) protocols and output signal after coupling for DPS (c) and DQPS (f). These results also prove that on receiver side protocols requirements are fulfilled for both DPS and DQPS. This opens possibility to introduce phase modulation as next research step.

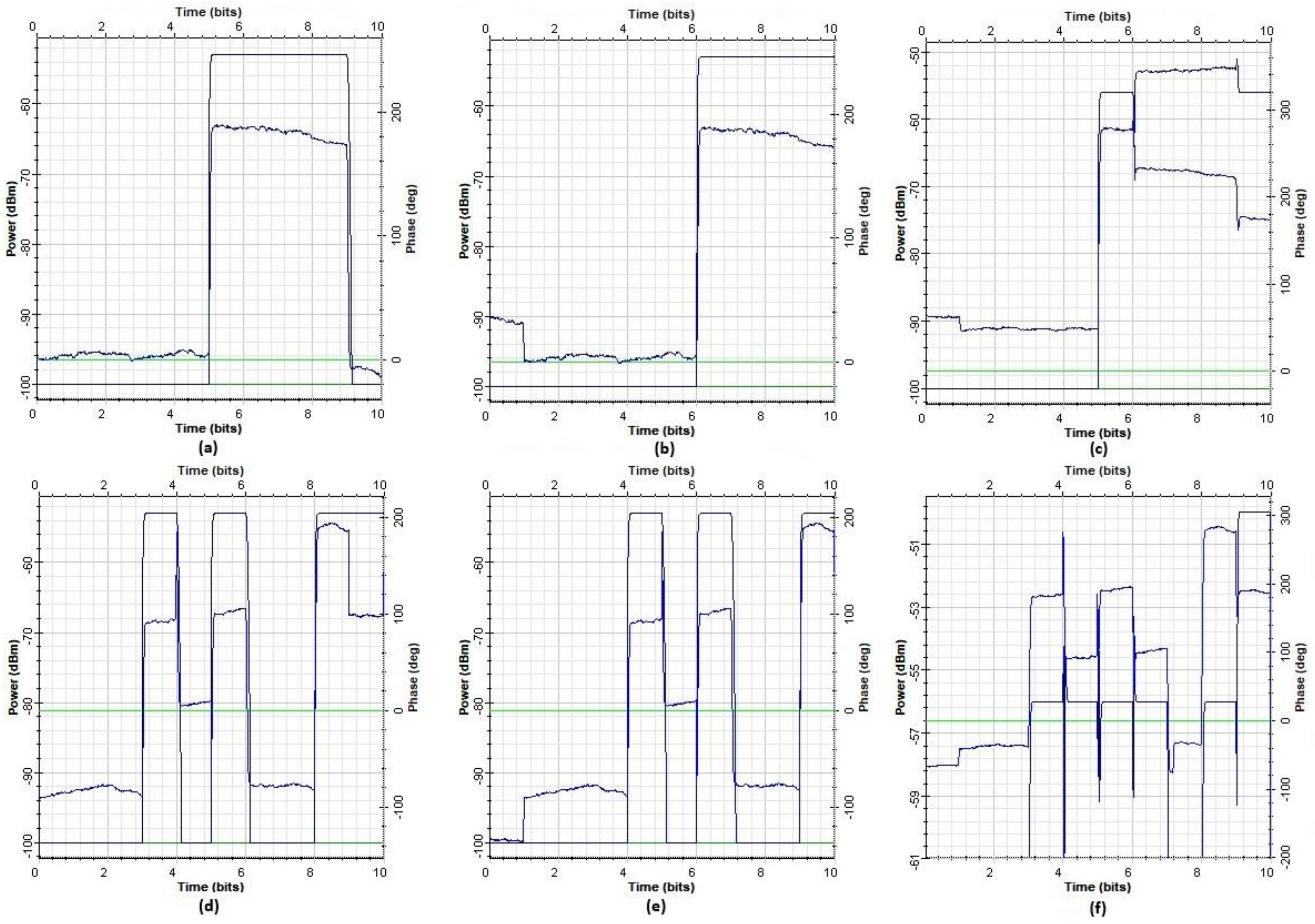


Fig. 3: Receiver output signal power and phase graphics measured for each receiver branch for both DPS (a), (b) and DQPS (d), (e) protocols and output signal after coupling for DPS (c) and DQPS (f).

CONCLUSION

In this poster we presented improved multiparameter QKD scheme aimed for authentication of both DPS and DQPS QKD protocols. We simulated three proposed schemes, solving synchronization problem. Presented simulation confirmed functionalities of both DPS and DQPS QKD protocols, their increased provable security level and gave us insight into improved performances of future QKD systems based on the proposed generalized optical QKD architecture. Those results are of utmost importance for implementation of mentioned QKD protocols and their integration within PON architecture.

REFERENCES

1. H. Takesue et al., 2008 First ITU-T Kaleid. Academ. Conf. 229-236 (2008).
2. N. Vokić et al., IEEE J. Sel. Top. Quant. Electron. 26, 3, 1-9 (2020).
3. N. Miljkovic et al., Opt. Quant. Electron. 50, 319 (2018).
4. https://www.itu.int/rec/T-REC-G.989.2

***ACKNOWLEDGEMENTS: This work was partially supported by the Serbian Ministry of Education, Science and Technological Development under contract No. 451-03-137/2025-03/200103.**